

# **A multi-protocol quantum key distribution transmitter**



**George Lloyd Roberts**

Department of Engineering  
University of Cambridge

This dissertation is submitted for the degree of  
*Doctor of Philosophy*



This thesis is dedicated to the memory of my grandfather, Alwyn Roberts.





## **Declaration**

I hereby declare that except where specific reference is made to the work of others, the contents of this dissertation are original and have not been submitted in whole or in part for consideration for any other degree or qualification in this, or any other university. This dissertation is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified in the text and Acknowledgements. This dissertation contains fewer than 65,000 words including appendices, bibliography, footnotes, tables and equations and has fewer than 150 figures.

George Lloyd Roberts

July 2018



## Acknowledgements

Firstly, I would like to express my gratitude to Andrew Shields and Richard Penty for giving me the opportunity to carry out research at Toshiba and Cambridge University. I am also grateful to my undergraduate supervisor, Mark Fox, for encouraging me to apply for this CDT programme.

I would also like to thank all the researchers at Toshiba. You have all made my time here better than I could have ever hoped for. Zhiliang for his constant guidance, immense knowledge and for being there whenever I needed help. I could not imagine having a better supervisor. Marco Lucamarini for always taking the time to help me understand the theory behind the experiments, for giving advice and for proofreading manuscripts. James Dynes for his technical advice and help when equipment wasn't working as it should. Also, my academic supervisor, Seb Savory, for continued support throughout my PhD and for showing me how the work fits in a classical communications perspective.

My four years at Cambridge have been the best of my life, owed in part to the amazing friends I have made here, of whom there are too many to list. A special mention goes to Stephen Geddis for the Lord of the Rings marathons, Michal for the fun times here and abroad, and Giacomo for being a proud Dwayne 'The Rock' Johnson fanboy with me. A big thank you so much to all my fellow students at Toshiba: Alex K-S and Bruno who have been with me from the start, Matt Anderson for sharing the cubicle with me, Mariella and Mirko for being better lab mates than I could have ever hoped for, Enzo for all the F1 and QKD chats and all others past and present: I would have been much less productive without all the coffee breaks! Also to all my friends from Woking (including, but not limited to): Matt Crawley, Mel Agnew, Stephen Rich and Alex Haley; from Sheffield: Gavin, Helen, Doug and Friis. I wouldn't be the person I am today without you.

I am grateful to my parents, Jane and Keith, for their unconditional love and support. My sister, Katie, who is one of the reasons I did my PhD in Cambridge. Also for giving me such a great brother-in-law. I am forever grateful to my Nanny, for all the talks and guidance whenever I needed advice, and to my Granny and Grandad, who always gave me so much love. I am also grateful to my many aunties, uncles, cousins and other family members who

have supported me along the way. A special gratitude goes to my partner, Cora, for her love and for being perpetually proud of my achievements. It would not have been the same without you.

# Publications

Parts of this thesis have been published in the following journals and talks have been given at international conferences.

## Journal publications

- “Directly phase-modulated light source”, *Physical Review X*, **6**, 031044 (2016).  
Z. L. Yuan, B. Fröhlich, M. Lucamarini, **G. L. Roberts**, J. F. Dynes, A. J. Shields.
- “Experimental measurement-device-independent quantum digital signatures”, *Nature Communications*, **8**, 1098 (2017).  
**G. L. Roberts**, M. Lucamarini, Z. L. Yuan, J. F. Dynes, L. C. Comandar, A. W. Sharpe, A. J. Shields, M. Curty, I. V. Puthoor, E. Andersson.
- “Modulator-free coherent-one-way quantum key distribution”, *Laser & Photonics Reviews*, **11**, 1700067 (2017).  
**G. L. Roberts**, M. Lucamarini, J. F. Dynes, S. J. Savory, Z. L. Yuan, A. J. Shields.
- “Manipulating photon coherence to enhance the security of distributed phase reference quantum key distribution”, *Applied Physics Letters*, **111**, 261106 (2017).  
**G. L. Roberts**, M. Lucamarini, J. F. Dynes, S. J. Savory, Z. L. Yuan, A. J. Shields.
- “A direct GHz-clocked phase and intensity modulated transmitter applied to quantum key distribution”, *Accepted by Quantum Science & Technology* (2018).  
**G. L. Roberts**, M. Lucamarini, J. F. Dynes, S. J. Savory, Z. L. Yuan, A. J. Shields.
- “Patterning-effect-free intensity modulator for secure decoy-state quantum key distribution”, *arXiv [quant-ph] preprint 1807.07414. Submitted to Optics Letters* (2018)  
**G. L. Roberts**, M. Pittaluga, M. Minder, M. Lucamarini, J. F. Dynes, Z. L. Yuan, A. J. Shields.

## Conferences

- “Experimental progress in measurement-device-independent QKD” Invited talk, Trustworthy Quantum Information, Shanghai, China, June 2016.  
M. Lucamarini, **G. L. Roberts**, L. C. Comandar, J. F. Dynes, B. Fröhlich, A. Plews, A. W. Sharpe, W. W.-S Tam, Z. L. Yuan, A. J. Shields.
- “Optically seeded lasers for quantum communication applications” Invited talk, Optics Frontier - Information Optics and Photonics, Shanghai, China, July 2016  
Z. L. Yuan, M. Lucamarini, **G. L. Roberts**, L. C. Comandar, B. Fröhlich, J. F. Dynes, A. W. Sharpe, A. Plews, W. W.-S Tam, R. V. Penty, A. J. Shields.
- “A modulator-free QKD transmitter” Contributed talk, QCrypt 2016, Washington DC, USA, September 2016.  
**G. L. Roberts**, Z. L. Yuan, B. Fröhlich, M. Lucamarini, J. F. Dynes, A. J. Shields.
- “Directly intensity-modulated quantum key distribution” Contributed talk, CLEO 2017, San Jose, USA, May 2017.  
**G. L. Roberts**, M. Lucamarini, J. F. Dynes, S. J. Savory, Z. L. Yuan, A. J. Shields.
- “Novel technologies for quantum key distribution networks” Contributed talk, IEEE Photonics Society Summer Topical Meeting Series, San Juan, Puerto Rico, July 2017.  
Z.L. Yuan, **G. L. Roberts**, J. F. Dynes, B. Fröhlich, M. Lucamarini, A. W. Sharpe, W. W.-S Tam, A. Plews, A. J. Shields.
- “Experimental demonstration of the differential quadrature phase shift protocol” Contributed talk, QCrypt 2017, Cambridge, UK, September 2017.  
**G. L. Roberts**, M. Lucamarini, J. F. Dynes, S. J. Savory, Z. L. Yuan, A. J. Shields.
- “Optical injection locking applied to quantum key distribution protocols” Contributed talk, SPIE Photonics Europe Quantum Technologies, Strasbourg, France, April 2018.  
**G. L. Roberts**, M. Lucamarini, J. F. Dynes, S. J. Savory, Z. L. Yuan, A. J. Shields.
- “Quantum key distribution enhanced by optical injection locking” Invited talk (and best paper prize), The Rank Prize Symposium on Challenges to Achieving Capacity in Nonlinear Optical Networks, Lake District, UK, June 2018.  
**G. L. Roberts**, M. Lucamarini, J. F. Dynes, S. J. Savory, Z. L. Yuan, A. J. Shields.

# Table of contents

<b>List of figures</b>	<b>xv</b>
<b>List of tables</b>	<b>xxiii</b>
<b>Nomenclature</b>	<b>xxv</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Cryptography . . . . .	1
1.1.1 Classical . . . . .	2
1.1.2 Quantum . . . . .	4
1.2 QKD protocols . . . . .	6
1.2.1 Discrete variable . . . . .	6
1.2.2 Distributed phase reference . . . . .	8
1.2.3 Continuous variable . . . . .	10
1.3 Practical QKD . . . . .	10
1.3.1 Key rates . . . . .	11
1.3.2 Channels . . . . .	12
1.3.3 Weak coherent pulses . . . . .	13
1.3.4 Phase modulation . . . . .	15
1.3.5 Phase demodulation . . . . .	17
1.3.6 Phase randomisation . . . . .	18
1.3.7 Finite-key-size analysis . . . . .	19
1.3.8 Single photon detectors . . . . .	19
1.3.9 Current state-of-the-art and future potential . . . . .	22
1.4 Motivation for research . . . . .	23
1.5 Novel contributions . . . . .	24
1.6 Organisation of thesis . . . . .	25

<b>2</b>	<b>A directly-modulated quantum light source</b>	<b>27</b>
2.1	Introduction . . . . .	27
2.1.1	Laser diodes . . . . .	27
2.1.2	Optical injection locking . . . . .	29
2.1.3	Pulse preparation . . . . .	32
2.2	System design and properties . . . . .	33
2.2.1	Transmitter design . . . . .	33
2.2.2	Gain switched laser pulses . . . . .	35
2.2.3	Spectra . . . . .	36
2.2.4	Interference contrast and visibility . . . . .	38
2.2.5	Phase modulation . . . . .	40
2.2.6	Practical phase randomisation . . . . .	42
2.3	Summary . . . . .	48
<b>3</b>	<b>Phase-modulated QKD</b>	<b>49</b>
3.1	Introduction . . . . .	49
3.2	Phase encoding . . . . .	49
3.3	Distributed phase shift . . . . .	50
3.3.1	Theory . . . . .	51
3.3.2	Directly-modulated implementation . . . . .	52
3.3.3	Results and discussion . . . . .	55
3.4	Differential quadrature phase shift and BB84 . . . . .	56
3.4.1	Theory . . . . .	58
3.4.2	Implementation . . . . .	59
3.4.3	Results and discussion . . . . .	63
3.5	Summary . . . . .	67
<b>4</b>	<b>Intensity-modulated QKD</b>	<b>69</b>
4.1	Introduction . . . . .	69
4.2	Intensity encoding . . . . .	69
4.3	Time-bin encoding . . . . .	70
4.4	Coherent one way QKD . . . . .	72
4.4.1	Theory . . . . .	72
4.4.2	Implementation . . . . .	74
4.4.3	Simulation . . . . .	77
4.4.4	Results and discussion . . . . .	78



---

4.5	Summary . . . . .	82
<b>5</b>	<b>Concurrent phase and intensity modulated QKD</b>	<b>83</b>
5.1	Introduction . . . . .	83
5.2	Phase and intensity encoding . . . . .	83
5.3	Theory . . . . .	85
5.3.1	Decoy states . . . . .	85
5.3.2	Secure key rates . . . . .	87
5.4	Implementation . . . . .	90
5.4.1	Directly-modulated decoy states . . . . .	90
5.4.2	Externally-modulated decoy states . . . . .	94
5.4.3	Concurrent phase and intensity modulation . . . . .	101
5.5	Results and discussion . . . . .	101
5.6	Summary . . . . .	106
<b>6</b>	<b>Future work</b>	<b>109</b>
<b>7</b>	<b>Conclusions</b>	<b>111</b>
	<b>References</b>	<b>115</b>



# List of figures

1.1	<b>Classical cryptography.</b> <i>(a) Identical encryption and decryption keys are used in symmetric cryptography. (b) Bob uses Alice's public key to encrypt the message in public key cryptography. Alice decrypts the message with her private key.</i>	3
1.2	<b>MDI-QKD with BB84.</b> <i>a) When Alice and Bob are both transmitting, MDI-QKD can be carried out. b) and c) When Alice or Bob are transmitting, BB84 can be carried out.</i>	9
1.3	<b>Poissonian number distributions.</b> <i>The probability of emitting <math>n</math>-photon pulses given the mean prepared photon number '<math>\mu</math>'.</i>	14
2.1	<b>Laser fundamentals.</b> <i>a) The three processes involving light in a laser gain medium. b) The inside of a DFB laser diode, where a periodic grating above the active medium only allows certain wavelengths to oscillate. Laser light exits through the port on the right.</i>	28
2.2	<b>Experimental setup.</b> <i>Directly-phase modulated transmitter design. LD=laser diode; Att=attenuator; EPC=electric polarisation controller; PBS=polarising beamsplitter; <math>\lambda</math>=wavelength filter. A circulator (with port numbers labelled) injects the light from the first LD into the second. Blue fibres are polarisation-maintaining, whereas yellow fibres are not.</i>	34
2.3	<b>Gain-switched laser pulses.</b> <i>Pulse profiles created by gain-switching the pulse preparation laser at 2 GHz. The DC bias is varied so the area under the pulses is similar with and without injection. The top two traces have no optical injection and are shown with and without a spectral filter. The bottom two traces have optical injection and are also shown with and without a spectral filter.</i>	35

2.4	<b>Unmodulated laser spectra.</b> <i>Unfiltered spectra for free running phase preparation and pulse preparation laser diodes as the pulse preparation laser wavelength is varied to provide different detunings. All lasers have a DC bias above their lasing threshold. The phase preparation laser spectrum is measured after attenuation to 50 <math>\mu</math>W. The detuning frequencies are 29.3 GHz, 24.5 GHz, -0.2 GHz and -28.9 GHz for panels a, b, c and d respectively. . . .</i>	37
2.5	<b>Gain-switched laser spectra.</b> <i>Unfiltered spectra for a gain-switched pulse preparation laser, with and without CW phase preparation laser injection (also shown). The AC voltage into the pulse preparation lasers is the same for both scenarios. The DC voltage is below threshold in both scenarios, however is higher without injection, to allow comparison in the plot. . . .</i>	38
2.6	<b>QBER origin.</b> <i>An AMZI is aligned to measure in one basis. Photons exiting through the bottom port are contribute to the QBER. . . . .</i>	39
2.7	<b>Master wavelength variation.</b> <i>The pulse preparation laser is gain switched at 2 GHz and the output properties are measured as 50 <math>\mu</math>W of CW light at different wavelengths is injected via a tuneable laser source. . . . .</i>	40
2.8	<b>Interference contrast.</b> <i>Evolution of the interference contrast with the injected seed power for a tuneable CW laser and a CW DFB laser diode. The pulse preparation laser is gain-switched at 2 GHz. Solid lines show the measured coherence of the phase preparation laser, whereas symbols show the system output with light injected into the pulse preparation laser. . . .</i>	41
2.9	<b>System concept.</b> <i>a) The frequency change, <math>\Delta\nu</math>, caused by a perturbation of length <math>t_m</math> to the driving signal, alongside b) the change in phase, <math>\Delta\phi</math>, compared to the original phase without the perturbation and c) the subsequent output pulses, with a phase modulation, but no change to the intensity or frequency. . . . .</i>	42
2.10	<b>Phase modulation.</b> <i>Shallow phase preparation laser modulations create arbitrary phase modulations in the system output measured using an oscilloscope. a) Optical response from the phase preparation laser; b) output from one arm of an AMZI. . . . .</i>	43
2.11	<b>Half-wave voltage.</b> <i>The phase shift between output pulses as a function of phase preparation laser modulation depth. . . . .</i>	43

2.12	<b>Injection-locked phase randomness.</b> <i>Phase randomness can be arbitrarily provided to pulses at 2 GHz by driving the phase preparation laser below threshold. a) Optical output from the phase preparation laser, showing depletion regions followed by peaks before a steady state region. The applied electrical signal has a down-time of 250 ps, whereas the optical down-time is around 200 ps. b) Colour-graded density plot of the output pulses after an AMZI.</i>	44
2.13	<b>Randomness histogram.</b> <i>Histograms of the random bits in a BB84 pattern for different down-times to break the phase coherence of the phase preparation laser. A simulation of the expected histogram is also given.</i>	47
2.14	<b>BB84 Autocorrelation.</b> <i>Inter-block interference only. The outer lines (red) show 99 % confidence bounds and the inner (blue) lines show 95 % confidence bounds.</i>	47
3.1	<b>Differential phase shift schematic.</b> <i>One method of implementing the DPS protocol uses a coherent pulse source (for example a carved CW laser) and a phase modulator, PM, to encode the relative phase, <math>\phi_i</math>, between pulses. After travelling through the quantum channel, Bob's receiver is a passive interferometer measuring signals in a single basis.</i>	51
3.2	<b>DPS oscilloscope traces.</b> <i>For cases where the signal is compensated and uncompensated. a) Electrical signal applied to the master laser. b) Optical signal from the master laser. c) Direct measurement of the optical system output. d) and e) Complementary outputs from both arms</i>	53
3.3	<b>DPS DC Compensation.</b> <i>The rolling average of pseudorandom <math>2^{10}</math>-bit patterns (top), with the measured intensity of every decoded pulse (bottom).</i>	54
3.4	<b>DPS bit intensity with AMZI phase.</b> <i>The peak intensity of the pulses is recorded by an oscilloscope as the AMZI is tuned about <math>3\pi</math>.</i>	55
3.5	<b>Experimental DPS results.</b> <i>Key rates and QBERs extracted using a transmitted mean photon number of 0.18 photons per pulse.</i>	56
3.6	<b>Potential BB84 transmitter.</b> <i>A phase-randomised pulse source sends pulses into an AMZI with a phase modulator (PM) on one arm. This produces pulse pairs with a globally random phase and a differential phase between the pair (<math>\phi_1, \phi_2</math>).</i>	57

3.7	<b>A Potential differential quadrature phase shift transmitter.</b> <i>An extra random number generator (RNG) is fed into the phase modulator (PM) to provide the random phases for blocks in the differential quadrature phase shift protocol. . . . .</i>	58
3.8	<b>BB84 master laser optical outputs.</b> <i>Measured optical waveforms for a 2 GHz (top) and 10 GHz (bottom) master laser, with a pseudorandom BB84 pattern input. The down-time is 250 ps. . . . .</i>	60
3.9	<b>DQPS blocks.</b> <i>Two example blocks for the DQPS protocol, with a block size <math>L=5</math>. This first pulse in all blocks is a reference pulse, hence only 8 useful bits are shown in the figure. . . . .</i>	61
3.10	<b>Differential quadrature phase shift schematic.</b> <i>Blocks of size <math>L=3</math> are injected into the slave laser via a circulator in this figure. At practical system efficiencies, the optimal block length used is longer than this. Bob's measurement values are shown along their respective pulse intensities when measuring in the <math>\pi</math> basis. . . . .</i>	62
3.11	<b>DQPS bit intensity with AMZI phase.</b> <i>The peak intensity of the pulses is recorded by an oscilloscope as the AMZI is tuned about <math>2\pi</math>. . . . .</i>	62
3.12	<b>DQPS and BB84 error rates.</b> <i>Measured QBERs at all experimental distances (symbols) shown alongside the simulated values (lines) based on the mean photon number used and the dark count rate. . . . .</i>	64
3.13	<b>DQPS and BB84 key rates.</b> <i>Secure key rates shown alongside the raw count rates for each protocol. Experimental data is given by symbols and simulated data based on the mean photon number are represented by lines. The DQPS block sizes, <math>L</math>, are also given. . . . .</i>	65
3.14	<b>DQPS and BB84 mean photon numbers.</b> <i>The optimum mean photon number for each protocol at different channel attenuations. . . . .</i>	66
3.15	<b>DQPS stability.</b> <i>The key rates and QBER for a continuous DQPS measurement at 8 dB channel attenuation with no active feedback. . . . .</i>	67
4.1	<b>QKD states on the Bloch sphere.</b> <i>The three potential QKD bases (X, Y and Z) are shown, with their states represented by arrows. <math>\phi</math> gives the phase encoding between the two pulses. . . . .</i>	71
4.2	<b>Potential COW implementation.</b> <i>This uses a coherent pulse source (for example a carved CW laser) and an intensity modulator, IM, to encode the bit value. . . . .</i>	73

4.3	<b>COW schematic.</b> A CW master laser is injected into a patterned gain-switched slave laser. Not shown are the filter and optical attenuator. This is then attenuated to the single photon level before being sent through the quantum channel to Bob. SPD <sub>1</sub> detects the time-bin encoded photons, and SPD <sub>2</sub> measures their visibility using a one bit asymmetric Mach-Zehnder interferometer (AMZI). The pattern shown in this figure is $ \beta_0\rangle$ , $ \beta_1\rangle$ , $ D\rangle$ , $ \beta_1\rangle$ .	75
4.4	<b>Bit intensity with AMZI phase.</b> The intensity of every bit after the AMZI is measured on an oscilloscope as the measurement basis is rotated about $2\pi$ .	76
4.5	<b>Measured COW SPD traces.</b> Signals received by bob in a) The Z basis; b) and c) the destructive and constructive arms of the X basis AMZI. The logical bit pattern shown, separated by vertical grey lines, is $ \beta_0\rangle$ , $ \beta_0\rangle$ , $ \beta_1\rangle$ , $ \beta_2\rangle$ , $ \beta_1\rangle$ , $ \beta_1\rangle$ , $ \beta_0\rangle$ , $ \beta_1\rangle$ . The acquisition time is 60 s, the quantum channel loss is 15 dB and Alice is transmitting 0.1 photons per pulse. . . . .	79
4.6	<b>COW error rates.</b> QBERs in the Z basis (top) and visibilities in the X basis (bottom). Experimental data is represented by symbols and theoretical data by lines. The theoretical analysis accounts for the increased detector jitter at short distances. . . . .	80
4.7	<b>COW key rates.</b> Experimental (symbols) and simulated (lines) key rates. The secure key rate is calculated using a finite-key-size analysis with a block size of at least $2 \times 10^7$ in the Z basis. . . . .	81
5.1	<b>Constellation diagrams.</b> Quadrature amplitude vs in phase amplitude for a) Amplitude shift keying, b) Quadrature phase shift keying and c) 8-quadrature amplitude modulation. Red circles indicate the modulation levels. . . . .	84
5.2	<b>Intensity and phase receiver.</b> The polar (Z) basis is measured with direct detection and the equatorial (X/Y) bases are measured using an AMZI with a phase modulator (PM) on one arm. This phase modulator is only necessary in some implementations. An attenuator (Att) is placed on the polar basis detection arm. . . . .	85
5.3	<b>Directly-modulated decoy-state schematic.</b> Six-state QKD with a lower driving level to directly produce decoy states. . . . .	91
5.4	<b>Slave signal ‘shelves’.</b> The pulses are shaped to minimise the effect of transient oscillations from the previous pulse. . . . .	91

5.5	<b>Directly-modulated decoy-state fluctuations without compensation.</b> <i>Intensity fluctuations of all pulses in a 4096-bit six-state QKD pattern when the decoy states are produced using direct modulation. The signal state has a value of <math>0.233 \pm 0.004</math>, whereas the decoy state has a value of <math>0.0955 \pm 0.014</math>. There are fewer decoy measurements than signal measurements due to the increased probability of Alice sending a signal state.</i>	92
5.6	<b>Directly-modulated decoy states spectra.</b> <i>Experimental results using a fixed 12 GHz spectral filter at 1550.08 nm. Both filtered and unfiltered spectra are normalised to have the same area.</i>	93
5.7	<b>Directly-modulated decoy states time offset.</b> <i>Traces of the signal pulse and the decoy pulse. The decoy pulse is offset by 500 ps.</i>	93
5.8	<b>Directly-modulated decoy state fluctuations with compensation.</b> <i>Intensity fluctuations when the decoy pulse overlaps perfectly with the signal pulse. The signal state has a value of <math>0.223 \pm 0.012</math>, whereas the decoy state has a value of <math>0.09428 \pm 0.029</math></i>	94
5.9	<b>Mach-Zehnder modulator.</b> <i>Schematic of a Mach Zehnder modulator with a coupling ratio R:T and a travelling wave phase modulator.</i>	95
5.10	<b>IM Response.</b> <i>Transmission (T) with voltage (V) for an interferometer-based intensity modulator. Power deviations for identical voltage shifts (<math>\Delta V</math>) at the peak (<math>\Delta P_2</math>) and quadrature point (<math>\Delta P_1</math>) are given. The red dotted line shows the output of a low extinction ratio interferometer.</i>	96
5.11	<b>Sagnac IM.</b> <i>Schematic of the Sagnac-based intensity modulator with a coupling ratio R:T.</i>	97
5.12	<b>Oscilloscope traces.</b> <i>The traces at the maximum ERs are shown for a random input pattern for three different beamsplitters.</i>	98
5.13	<b>Temporal stability.</b> <i>The output power from an unmodulated Mach Zehnder intensity modulator and the 80:20 Sagnac intensity modulator with no feedback. The power is normalised so the maximum power output is unity.</i>	100



- 5.14 **Six directly-modulated states traces.** *Measurement traces without decoy state preparation and basis intensity equalisation. The Z basis (top) has only a single trace, whereas the X and Y bases (middle and bottom) each have two AMZI outputs. The corresponding input pattern values are displayed at the top, labelled as Bb, where B is the basis and b is the logical bit value inside that basis. A red (grey) peak in the X and Y bases correspond to a ‘0’ (‘1’) logical bit, where the photon exits through the upper (lower) AMZI port. Peaks in output 1 (2) of the AMZI are complemented by small counts in output 2 (1) (middle inset), showing the high distinguishability between bits.* 103
- 5.15 **Experimental counts and error rates.** *The raw counts for each matched basis and intensity for the 20 minutes acquisition time (top) and the corresponding measured QBER (bottom). Lines give the simulation results, stars give the experimental results in real fibre and all other symbols give the experimental results with an attenuator as the optical channel. . . . .* 104
- 5.16 **Polar BB84 Results.** *Secure key rate (SKR) in the asymptotic (filled symbols, dotted line) and finite-key-size regimes (empty symbols, solid line). The star corresponds to data collected with real fibre as the quantum channel. . . .* 105
- 7.1 **All protocols key rates.** *Asymptotic secure key rates for all QKD protocols implemented in this thesis. . . . .* 113



# List of tables

1.1	<b>Example BB84 protocol key exchange.</b> $\uparrow$ corresponds to the rectilinear basis ( $H=0$ , $V=1$ ) and $\nearrow$ to the diagonal basis ( $D=0$ , $A=1$ ). The post sifting result is false if the bases are mismatched. . . . .	5
1.2	<b>State of the art SPDs</b> at 1550 nm. TES: transition edge sensor; SD-SPAD: self-differenced SPAD. . . . .	22
4.1	<b>Direct patterning effects.</b> The signal ('s') pulse intensities extracted from a $2^9$ -bit pseudorandom pattern input to the pulse preparation laser proceeding either another signal or a vacuum ('w') state. The average 's' pulse intensity is normalized to unity. . . . .	76
5.1	<b>External patterning effects.</b> The pulse intensities extracted from a $2^{10}$ -bit pseudorandom pattern input to Sagnac intensity modulators with three different beamsplitting ratios when preceded by a decoy pulse ('v') or another signal pulse ('s'). The average 's' pulse intensity is normalised to unity for each beamsplitter. . . . .	99



# Nomenclature

## Acronyms / Abbreviations

ACF	Autocorrelation function
AMZI	Asymmetric Mach-Zehnder interferometer
APD	Avalanche photodiode
ASK	Amplitude shift keying
AWG	Arbitrary waveform generator
B92	Bennett 1992
BB84	Bennett Brassard 1984
BS	Beamsplitter
COW	Coherent one way
CV	Continuous variable
CW	Continuous wave
DFB	Distributed feedback
DPR	Distributed phase reference
DPS	Differential phase shift
DQPS	Differential quadrature phase shift
DV	Discrete variable
E91	Ekert 1991

---

EAM	Electroabsorption modulator
EPC	Electric polarisation controller
ER	Extinction ratio
LD	Laser diode
MDI	Measurement-device-independent
MZM	Mach-Zehnder modulator
OIL	Optical injection locking
PBS	Polarising beamsplitter
PLC	Planar lightwave circuit
PRNG	Pseudorandom number generator
PSK	Phase shift keying
QAM	Quadrature amplitude modulation
QBER	Quantum bit error rate
QKD	Quantum key distribution
QRNG	Quantum random number generator
RF	Radio frequency
RNG	Random number generator
SD	Self differenced
SNSPD	Superconducting nanowire single photon detector
SPAD	Single photon avalanche photodiode
SPD	Single photon detector
TES	Transition edge sensor
TF-QKD	Twin field QKD

# Chapter 1

## Introduction

Communication has been essential to the development of mankind and has paved the way to incredible human achievements. In the 1800s, communication over long distances, or telecommunication, became feasible due to the invention of the telegraph and then the telephone. These devices enabled the transmission of information through conducting materials such as copper, by encoding data on electrical signals. The transmission distance and amount of information that can be sent this way is limited because the lines are lossy and are potentially noisy due to interference [1, pp. 1–4].

Optical fibres can be used instead, carrying data as light. These are flexible cables with a dielectric core for light to travel through, surrounded by a dielectric cladding material with a smaller refractive index. Light is guided down this waveguide, allowing signals to be sent and received with a small loss, due only to scattering and absorption in the fibre [1, pp. 4–8]. They became especially useful in the 1980s due to the development of semiconductor lasers and light emitting diodes. These can efficiently produce light in the low-loss regions of glass, allowing for a standard transmission loss rate of 0.2 dB/km at a light wavelength of 1550 nm. Today, there is a vast network of optical fibre links all around the world, enabling high-speed and high-bandwidth telecommunication.

### 1.1 Cryptography

It is often important for two parties, Alice and Bob, to communicate in private. An eavesdropper, Eve, can listen to signals sent through a copper cable by placing electrical coils around the cable and observing the leakage. She can also eavesdrop signals sent through optical fibres, where she simply bends the fibre to the extent that light leaks out [2]. This allows her to extract some of the signal, giving her information about the message, whilst leaving

her intrusion unnoticed. This is worrying, because without countermeasures it would mean that highly sensitive information is not private. Patient data transmitted between hospitals, sensitive military details or government communications could be read by malevolent parties.

Cryptography is the study of how to ensure data transmitted through a communication channel remains confidential. It also explores authentication, which means the receiver can be certain that a message is sent from the correct person; integrity, which ensures the message is not tampered with; and non-repudiation, which prevents a party from pretending that they did not send a message [3, pp. 2–4]. Confidentiality is enabled by encryption, where an algorithm is used to obscure the contents of a message from any nefarious third parties. If these third parties learn how to decipher messages with a certain algorithm, cryptographers must fix the algorithm or use a new one. This competition has created a cycle of continuous improvement across centuries.

The importance of the field has led to it drawing sustained interest from monarchies, governments, companies and individuals. It is thought to have been conceived over 4000 years ago, where a secret form of hieroglyphics was stored inside the Great Pyramid in Egypt [4]. From then, it has been famously used by, amongst many other examples, Spartan informants inside the Persian army, Mary Queen of Scots as part of an assassination plot on Queen Elizabeth I, and by all militaries in the Second World War [5].

### 1.1.1 Classical

#### Encryption

Encryption is where the contents of a message are obscured by applying a key to the message. Only someone with the decryption key can extract the original message. Rudimentary encryption can be done by hand, however the World Wars saw a rapid development of encryption algorithms and hardware. This led to advanced hardware being used, such as rotor machines, to perform cryptography. Nowadays it is completely automated by computers, allowing nearly everyone to implement some form of encryption on their communications. There are two main types of cryptographic encryption, public key cryptography and symmetric encryption [3], as shown in Fig. 1.1.

In public key cryptography, Alice generates a public key from a private key using a one-way function [6]. This mathematical function should make it impossible to derive the private key from the public key. In this way, Alice can distribute her public key to Bob, who can use it to encrypt his message. Alice is the only party with the private key, hence only she can decrypt the message. It has not yet been possible, however, to mathematically prove



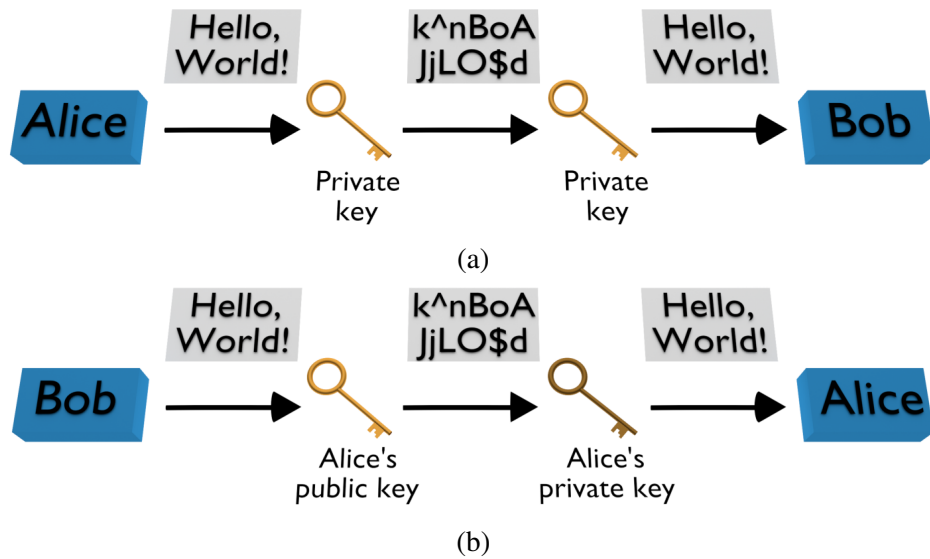


Fig. 1.1 **Classical cryptography.** (a) Identical encryption and decryption keys are used in symmetric cryptography. (b) Bob uses Alice's public key to encrypt the message in public key cryptography. Alice decrypts the message with her private key.

the existence of a perfect one-way function. Indeed, RSA is a current implementation of public key cryptography and is considered secure [7, 8]. This is based on it being simple to calculate the product of two large prime numbers, but very difficult to determine the original prime numbers given the product. Unfortunately, a working quantum computer would allow RSA encryption to be broken in a realistic timescale by using Shor's algorithm to efficiently factorise the product [9]. This is a worrying prospect because a large amount of data that is currently considered secure could be decrypted in the future.

Symmetric encryption is where Alice and Bob share an identical key for both encryption and decryption. This can be implemented using a block cipher or a stream cipher [10, pp. 98–100]. Block ciphers separate the message into sections, for example a 256-bit block, each of which is encrypted using the same key. Stream ciphers combine the message with a pseudorandom (or random) key, meaning each bit in the message is treated separately. Stream ciphers can be made completely secure if the key is perfectly random and is discarded after use. This is known as a Vernam cipher, or one-time pad. Reusing the key, or using a non-random key, gives information to Eve. The difficulty with this, however, is in how to initially distribute the key between the two parties. Public key methods, such as RSA, can be used once at the beginning of the communication to exchange a private key, then the message can be encrypted with symmetric encryption. Unfortunately, this does not address the security concern of public key cryptography. An eavesdropper could hack the initial

public key exchange and subsequently gain access to the entire message. A workaround is to use large block sizes that would take a long time to factorise, even with a quantum computer, however this is not future-proof and assumes that a more efficient algorithm will not be devised to calculate the private key. One secure method is to use a courier to physically exchange the key, however this is not always possible and will require more meetings when the keys are used up.

### 1.1.2 Quantum

Quantum key distribution (QKD) is a method that promises to solve the key exchange issue in symmetric cryptography, sidestepping the potential insecurity of public key cryptography [11, 12]. This technique, proposed in 1984 [13], exploits the principles of quantum mechanics to detect if anyone is eavesdropping on the signal transmission. This allows the users to share a perfectly secure one-time pad. To do this, Alice sends a single qubit, usually a photon, to Bob. A qubit is the quantum version of a classical bit, where, instead of being either 0 or 1, a particle is in a superposition state of the two values. If Eve attempts to measure the qubit, she will disturb it in a manner observable to the communicating parties because she collapses the state into one of the measurement values. If Alice and Bob see that someone is listening to their key exchange, they can simply choose not to use that key for encryption. QKD is based on the fundamental laws of physics, ensuring it is future-proof when implemented correctly. This means that someone eavesdropping on the message transfer will never be able to decrypt the message, even with infinite computational power.

The security of QKD is commonly and intuitively related to Heisenberg's uncertainty principle. This states that two conjugate properties of a particle cannot be known together, for example its position and momentum. If one property is measured with absolute precision, the other property of the particle becomes non-deterministic. QKD also relies on the no cloning theorem outlined by Wootters and Zurek (1982) [14], which shows that a quantum state cannot be perfectly replicated. This prevents an attacker from cloning a photon and measuring the quantum state of the clone.

Bennett Brassard 1984 (BB84) was the first QKD protocol to be proposed and is perhaps one of the simplest to help understand the basics of the technology. Let's assume that Alice is using polarisation to encode information on single photons of light. She chooses two potential bases to encode data in, each with orthogonal states within the basis. These states correspond to the bit value. The rectilinear basis contains horizontally (H) and vertically (V) polarised photons, and the diagonal basis contains diagonally (D) and anti-diagonally (A)

polarised photons. She randomly, and without bias, chooses a basis and bit to encode each photon she transmits to Bob. Bob then randomly selects a basis (H-V or D-A) to measure each received photon. In an ideal system, when Bob measures in the same basis as Alice's encoding basis, he will always measure the same bit that Alice transmitted. If he chooses the wrong basis, however, the result is non-deterministic because the bases are conjugate. This means that results obtained using mismatched bases must be removed. To do this, Alice communicates her encoding basis for all of Bob's clicks, allowing them to share an identical key. An example of this is shown in Table 1.1.

**Table 1.1 Example BB84 protocol key exchange.**  $\uparrow$  corresponds to the rectilinear basis ( $H=0$ ,  $V=1$ ) and  $\nearrow$  to the diagonal basis ( $D=0$ ,  $A=1$ ). The post sifting result is false if the bases are mismatched.

<b>Alice Basis choice</b>	$\nearrow$	$\nearrow$	$\uparrow$	$\nearrow$	$\uparrow$	$\uparrow$	$\nearrow$	$\uparrow$
<b>Alice Sent Bit</b>	0	1	1	0	0	0	0	1
<b>Bob Basis Choice</b>	$\uparrow$	$\nearrow$	$\nearrow$	$\uparrow$	$\uparrow$	$\nearrow$	$\nearrow$	$\uparrow$
<b>Measured Bit</b>	1	1	1	0	0	1	0	1
<b>Post Sifting Result</b>	x	✓	x	x	✓	x	✓	✓
<b>Agreed Key</b>	-	1	-	-	0	-	0	1

The situation changes if an eavesdropper is present. Like Bob, Eve must also choose a measurement basis, which she will get wrong 50 % of the time (assuming each basis is equally likely to be sent by Alice). Because the bases are conjugate, this means she has an overall 25 % chance of measuring a different bit to the one prepared by Alice. She then sends her measured state in her measurement basis to Bob. Her errors are directly transferred to Bob, meaning that even when Alice and Bob choose the same basis, they could measure different bit values due to Eve measuring in the incorrect basis. Alice and Bob compare a subset of their keys to measure the error rate, allowing them to identify if there is an eavesdropper in their quantum channel.

Even without an eavesdropper in the channel, Alice and Bob's keys will not be identical after removing measurements in mismatched basis. This is due to noise in the system that can come from a number of sources, for example imperfect state encoding or detector dark counts. These noise sources are unavoidable, hence algorithms are used to remove errors and ensure Alice and Bob share identical keys. A maximum tolerated error rate is defined by the QKD protocol, above which distilling a secure key is impossible.

## 1.2 QKD protocols

Since 1984, a number of different QKD protocols have been developed, each with strengths and weaknesses that make them more or less useful in different circumstances. The more prominent protocols are briefly discussed in this section, and those implemented in this thesis are described in more detail in their corresponding chapters. Regardless of the protocol used, all will result in Alice and Bob sharing an identical random key. Ideally, the protocols should be simple to implement, provably secure, enable a high bit rate, and work over long distances. The protocols fit into three main categories [12]:

- Discrete variable (DV) QKD encodes information on separate qubits. These protocols require single-photon detection techniques.
- Distributed phase reference (DPR) protocols are a variant of DV QKD but have major theoretical differences so are treated separately. These protocols exploit the coherence between neighbouring time bins, so the quantum state is a tensor product over a number of individual photon wavefunctions.
- Continuous variable (CV) QKD encodes information on the phase and amplitude quadrature of the optical field, and thus can be detected by homodyne or heterodyne techniques.

There are three different kinds of attack that are interesting when discussing QKD. The first, and weakest, is an individual attack. Here, Eve entangles quantum probes with each of the photons separately, stores them in a quantum memory until after Alice and Bob have communicated classically, then measures each probe individually. The second is a collective attack. Here, Eve entangles quantum probes with each of the photons separately, stores them in a quantum memory, then performs a single measurement on the entire system using a quantum computer. The final, and most general, is known as a coherent attack. In a coherent attack, Eve entangles a large quantum probe with all of the photons, stores the probe in a quantum memory, then can perform any measurement that is allowed by quantum physics on the probe.

### 1.2.1 Discrete variable

DV protocols encode information on qubits, which relies on phase/intensity or polarisation encoding of single photons. These protocols were the first to be introduced and are therefore the best developed class of protocols. Security has been proven for a number of DV protocols

against the most general form of attack, and very high secure key rates have been achieved with this security. BB84 is one example of a DV QKD protocol. B92 is a development of BB84 that uses just two states, instead of the four in BB84 [15]. Each state is in a different basis, making the protocol easier to experimentally implement, although the security is weaker, leading to lower secure key rates [16]. Two other interesting DV QKD protocols are detailed below.

## **E91**

Some protocols are based on photon entanglement [17, 18]. Entanglement is the physical phenomenon observed when two photons are linked such that an action on one photon will affect the other photon. The photons are initially in superposition states. When one photon is measured, the wavefunctions of both particles collapse, yielding results that are correlated. The use of entanglement to communicate between parties is known as quantum teleportation [19].

The Ekert 1991 (E91) protocol, named after Artur Ekert, uses entangled photons [20]. This protocol can be carried out with any party (Alice, Bob or Charlie) distributing a pair of entangled photons to Alice and Bob. The distributing party prepares superposition states, so has no knowledge of what the measured state will be. Alice and Bob randomly select a basis to measure each bit in and then sift their bits, as in other protocols.

To test the security of the link, they choose another basis in which to measure the incoming bits and measure Bell's inequality. This does not hold for entangled particles, and thus they can tell if the particles have been interfered with. An advantage of this protocol is that the random number generation is inherent to the state detection. This removes the need for high speed quantum random number generators. A downside is that entangled photon sources are not very bright, limiting the key rates [21].

## **Measurement device independent QKD**

When analysing a QKD system, quantum hackers will look to the most complex part of the system first, because this is the most likely to contain vulnerabilities. In the case of DV QKD, the detector has the most complexity, so most attacks target Bob's detectors [22, 23, 24]. For example, Eve shines light into Bob's detectors in the blinding attack so that his single photon avalanche photodiodes (see Section 1.3.8) are operating in the linear regime, rather than the Geiger regime. This allows her to control them by sending in her own light pulses. She can then ensure that Bob's detectors only click when he measures in the same basis as her, giving

her full key information and introducing no errors. Measurement-device-independent (MDI) QKD removes all detector vulnerabilities by introducing another party in the communication, Charlie [25, 26, 27]. Charlie is the only person with detectors, and learns nothing about the key shared between Alice and Bob.

The role of Charlie in this protocol is to perform a Bell state measurement on the states from Alice and Bob. A two-qubit system has four possible Bell states that represent maximal entanglement between the qubits, and a Bell state measurement projects the system onto one of these Bell states. If Alice knows the state of her particle and which Bell state Charlie measures, she can infer what state Bob prepared. Charlie performs this measurement by interfering the incident photons from the two communicating parties using a beamsplitter (BS). Identical photons with a random phase incident in the same polarisation state will exit via the same arm of the BS due to the Hong Ou Mandel effect [28, 29]. Each output of the BS then has an identical polarising BS with single photon detectors (SPDs) at each output, giving a total of four detectors. Charlie communicates to Alice and Bob every time he measures a coincidence between detectors. Alice and Bob are able to infer a shared key because which detectors click tell them the parity of the combined photons. Each party knows the state they encoded, thus also knows the state the other party encoded. Charlie would have to know Alice or Bob's initial states in order to know each bit, thus he gains no information in this procedure and can even be completely untrusted.

The author of this thesis has also published an experimental demonstration of how MDI-QKD can be carried out alongside BB84 [30]. Here, a 45 degree polarisation rotator is placed on one output of the BS in Charlie, allowing measurements in both polarisation bases. To carry out BB84 with Charlie, Alice *or* Bob should transmit a qubit. To carry out MDI-QKD with one another, Alice *and* Bob should transmit a qubit. A schematic of this is shown in Figure 1.2. This could be quite an important development for quantum networks, allowing all users to be linked securely with  $N - 1$  physical links, rather than the  $N(N - 1)/2$  physical links that would be required in an ordinary QKD network. It also means that the average consumer needs only a transmitter, the cheapest component in QKD systems, relying on an untrusted company or government to act as Charlie with the expensive detectors.

### 1.2.2 Distributed phase reference

The first distributed phase reference protocol was proposed in the early 2000s as a method of simplifying DV QKD experiments [31]. DPR protocols, unlike DV protocols, use a series of coherent states, meaning the coherence is maintained across all pulses. This makes them

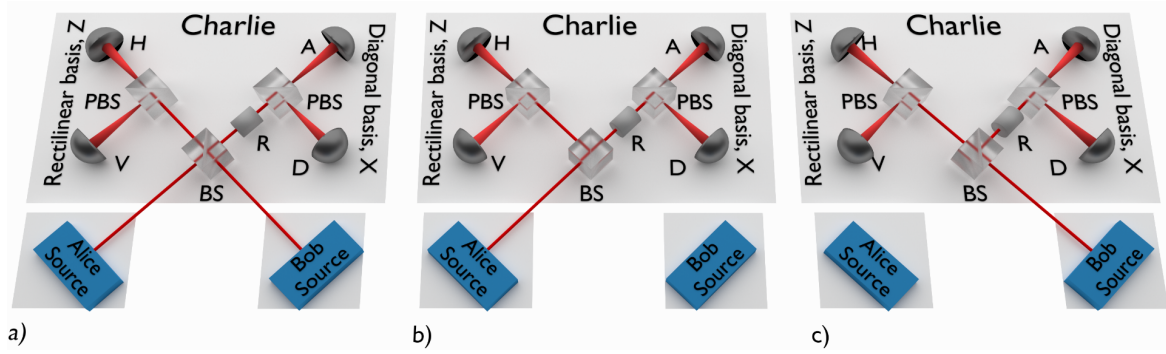


Fig. 1.2 **MDI-QKD with BB84.** *a) When Alice and Bob are both transmitting, MDI-QKD can be carried out. b) and c) When Alice or Bob are transmitting, BB84 can be carried out.*

simpler to implement because no phase randomisation is required. A break in the coherence signifies that Eve has made a measurement, allowing Bob to monitor the channel for her presence. Three different DPR protocols are implemented in this thesis, therefore a detailed discussion of how each protocol works is left to their respective chapters.

Whilst there are a number of methods to prove the security of DV protocols it is more difficult to derive a general security proof for DPR protocols because of the way the photon wavefunction is spread over a number of time bins. Security proofs must instead be studied for specific attacks [32, 33, 34, 35, 36]. Fortunately, the class of protocols is inherently secure against photon number splitting attacks, which can severely reduce the secure key rate of DV protocols. This attack is detailed in Section 1.3.3. The inherent security of DPR protocols is because an eavesdropper introduces errors in the phase when she tries to do a measurement on the pulses. This means that the attack is no longer a zero error attack and Alice can send a higher mean photon number than in conventional BB84, leading to a higher secure key rate.

Although their resilience to photon number splitting attacks means that DPR protocols perform better than many DV protocols, it comes at a cost. The security of DPR protocols has not been proven against coherent attacks, meaning there is currently no absolute lower bound for the key rate. Whilst actually implementing a coherent attack seems completely inconceivable, the aim of QKD is often to provide ‘unconditional’ security, rather than just ‘practical’ security. In key rate equations for DPR protocols, Eve’s information is estimated based on her most effective attack.

### 1.2.3 Continuous variable

Cryptography using continuous variables relies on the quadrature components of a light field,  $x$  and  $p$ . It is impossible to measure  $x$  and  $p$  simultaneously because they are non-commuting [37]. Quadrature amplitude modulation can be achieved by independently modulating two light beams that have a 90 degree phase shift between them. The combination of the two creates a single beam with information contained in both the amplitude and phase quadratures. Measurement is performed using balanced homodyne detection, where the quantum signal is interfered with a classical reference signal at a beamsplitter and the difference between the two beamsplitter outputs is measured. The phase of the reference signal determines which quadrature is measured [38].

The main advantage this technique holds over DV-QKD is that the balanced homodyne detectors are similar to those in existing telecommunication systems using coherent detection [39]. This means that developing the kind of detectors required for practical CV-QKD is more simple than in DV-QKD. Many drawbacks exist for this technique, however. The largest bottleneck is that CV-QKD does not have any clock periods with no detections, meaning the received signal requires heavy post processing for error correction [40]. This limits the secure key rate that can be extracted in a practical scenario. The secure key rate that can be extracted is also heavily dependent on the excess noise, a parameter that describes all noise sources beyond the vacuum noise, for example imperfect modulation, phase fluctuations and detector noise [41, 42, 43]. This prohibits secure keys from being distributed over long distances. Finally, although there has been continued research in this direction, no finite-key-size security proof has been derived for CV-QKD against coherent attacks, making it an important direction of research [43, 44]

CV-QKD has been demonstrated with a secure key rate of 1 Mbps over 25 km of optical fibre [45]. This is made possible by minimising the excess noise using coarse wavelength division multiplexing to separate the quantum and classical reference signals, and by using highly efficient low-noise 1 GHz shot-noise-limited homodyne detectors. This group has used the same technology to provide the record distance for CV-QKD, over 100 km of optical fibre, giving a secure key rate just below 1 kbit/s [46].

## 1.3 Practical QKD

The theoretical analyses of DV and DPR protocols must be translated into real world scenarios, whilst ensuring security is still maintained. Real QKD systems, for example, have errors



which must be dealt with. Some features, terms and equations are common to all protocols, and these are explained in this section. The final secure key rate that can be extracted from raw detection events at Bob, as well as the requirements on the channel linking Alice and Bob and the single photon sources that can be used are detailed. Also, methods of phase modulation, demodulation and randomisation, the practical effect of having a finite key length to extract error rates from and the current state-of-the-art of the field are outlined.

### 1.3.1 Key rates

For QKD experiments, the following expression can be written for the detection probability in each clock period measured by Bob,  $P_{click}$ :

$$P_{click} = \mu \eta_{channel} \eta_{det} + P_{dark}, \quad (1.1)$$

where  $\mu$  is the transmitted photon number,  $\eta_{channel}$  is the channel transmissivity,  $\eta_{det}$  is the detection system efficiency, and  $P_{dark}$  is the dark count probability. In optical fibres (with a loss rate of  $\alpha$  dB/km) the channel loss can be related to the channel length in km,  $L$ , by

$$\eta_{channel} = 10^{-\alpha L/10}. \quad (1.2)$$

The error rate probability, or quantum bit error rate (QBER), is an important parameter that allows the users to estimate how much information Eve can have. It is defined as the ratio of incorrectly measured bits to the total number of measured bits [47]. One contribution to this is the base error rate ( $QBER_{base}$ ), which can be caused by imperfect modulation and optical misalignment. Another contribution is the dark counts, which have a random probability of making the wrong detector click ( $P_{dark}$ ). This dependence causes the QBER to increase at long distances, limiting the maximum distance over which secure keys can be generated. These quantities are combined in the following expression [48]:

$$QBER = QBER_{base} + \frac{P_{dark}}{2P_{click}} \quad (1.3)$$

The factor of two comes from the fact that dark counts have a 50 % probability of causing the correct detector to click in a system with two detectors. A phenomenon observed in some SPDs, afterpulsing, as described in Section 1.3.8, can also increase the QBER.

After Bob has detected the qubits transmitted by Alice, their raw keys will be different, meaning they must do post-processing to extract identical keys and to ensure that Eve has no

information about the key. The first step is sifting, in which the two parties compare their transmission and measurement basis, alongside Bob informing Alice when he measured a ‘click’ in his detectors. They then discard any bits in mismatched bases. The next step is error estimation, where they take a subset of their keys for comparison so they can calculate the QBER. If this error is too high, they should not use the key. Next is error correction. Here, Alice and Bob run an algorithm over the public channel to ensure their keys are identical. A number of methods of doing this exist, with varying efficiencies due to removal of non-erroneous bits and computational efficiencies (i.e. speed). Finally, the two parties run a privacy amplification protocol. This reduces Eve’s information about the key,  $I_E$ , to zero. This also has a finite efficiency, removing more bits than Eve could have possibly obtained.

The secure key rate per bit,  $R$ , can be written as

$$R = I_{AB} - I_E, \quad (1.4)$$

where  $I_{AB}$  is Alice and Bob’s mutual information and  $I_E$  can be related to Alice (Bob) and Eve’s mutual information,  $I_{AE}$  ( $I_{BE}$ ):

$$I_E = \min(I_{AE}, I_{BE}). \quad (1.5)$$

$I_{AB}$  concerns the error correction using the QBER estimated from the majority basis.  $I_E$  pertains to the privacy amplification using the QBER estimated from the minority basis. This is the same for all protocols, and thus some permutation of this will be seen in all secure key rate equations.

### 1.3.2 Channels

QKD systems require a channel capable of transmitting qubits. An obvious solution is free-space, although ground-based links are distance and weather limited because a line of sight between the transmitter and receiver is required [49, 50, 51]. Other drawbacks include sensitive alignment, noise due to air currents and also the sensitivity of the single photon detectors to background light. Satellite QKD can enable drastic improvements in the distances secure keys can be exchanged over because there is negligible photon loss and no atmospheric turbulence in space [52]. The major drawback to this technique is the extreme cost and poor availability.

Optical fibres provide a good alternative to free-space QKD. The loss is relatively low, and no new infrastructure is required because ordinary fibre optic cables can be used. It is

also very easy to connect transmitters and receivers to fibre optics due to standardisation of the technology in classical communications.

Two links between Alice and Bob are required for secure QKD [12]. These can be the same physical channel if techniques like wavelength division multiplexing are used [53, 54]. The first link is an untrusted quantum channel that the qubits are sent through. Untrusted here means that an eavesdropper can do whatever she wants to the qubits. The second link is a public authenticated channel. Anybody can read the information in this channel, however the authentication means that only Alice and Bob can transmit information to each other in the channel because the messages contain their signatures.

### 1.3.3 Weak coherent pulses

QKD would be best implemented with a high-rate ideal single photon source. Ideal in this case means that there is a 100 % probability of emitting just one photon in each clock period. Also, this should be within the low-loss windows for optical fibres to allow for the best scaling with distance. Single photons can be produced deterministically in many ways, from semiconductor quantum dots to nitrogen vacancy centres in diamond. Unfortunately no ideal source has been developed and, more importantly, the current high-rate single photon sources are not efficient at the low-loss windows in fibre-optic cables. Indeed, QKD has been carried out with a quantum dot, however its efficiency makes the secure key rates generated poor [55].

In practice, weak coherent pulses are found to perform much better than single photon sources [56, 57, 58, 59]. These are classical light pulses that are attenuated down to contain a small mean number of photons,  $\mu$ , and obey a Poissonian number distribution, where the probability of emitting an  $n$ -photon state is

$$P(n) = \frac{\mu^n}{n!} e^{-\mu}. \quad (1.6)$$

This technique also has the benefit of being easy to implement with current telecommunications technology.

An example of two such Poissonian distributions for mean photon numbers of 0.5 and 0.1, is given in Fig. 1.3. This shows that the most probable outcome for both cases is that Alice emits no photons. Equally, there is some probability of each emission containing multiple photons, opening the door to a simple attack by Eve, known as a photon number splitting attack. In this attack, an all powerful Eve performs a quantum non-demolition measurement on Alice's pulses as they travel through the quantum channel, so she can identify the number

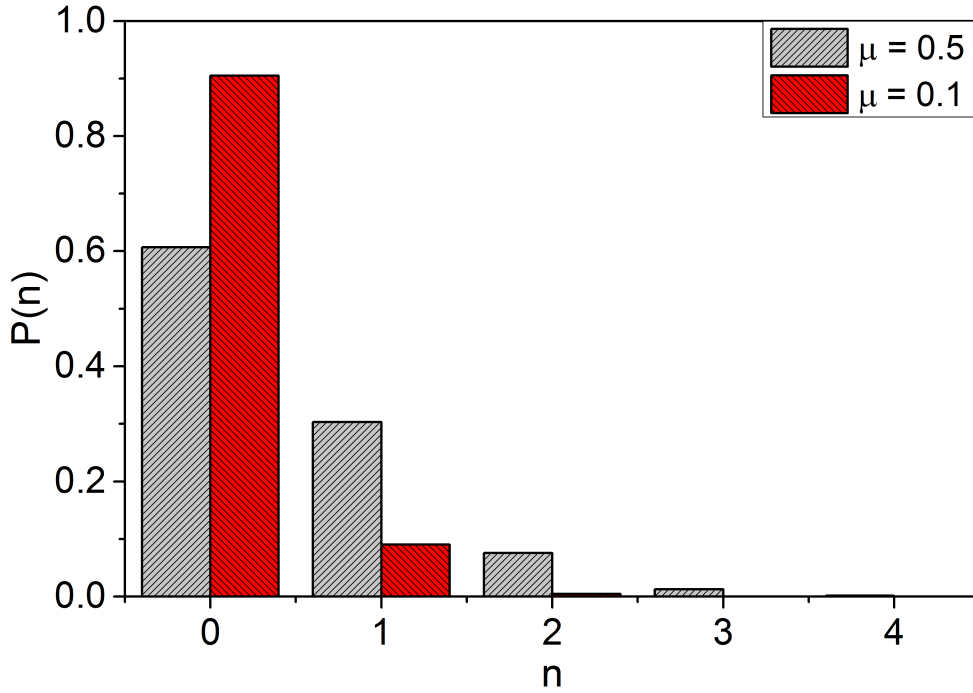


Fig. 1.3 **Poissonian number distributions.** *The probability of emitting  $n$ -photon pulses given the mean prepared photon number ' $\mu$ '.*

of photons in each pulse. She extracts one photon from each multi-photon pulse and stores it in her quantum memory, then blocks all the single photon pulses. Subsequently, she listens to the classical basis reconciliation between Alice and Bob, allowing her to obtain identical measurement results to Bob on her stored photons. With this technique, Eve can obtain full knowledge of the key without introducing any errors. For this reason, it must be assumed that every time Bob measures a click in his detectors, it could have originated from a multi-photon pulse transmitted by Alice and hence is considered completely insecure. It is worth noting that this attack is only possible because no restrictions are placed on Eve. In reality, Alice and Bob could simply postpone their basis reconciliation to a time beyond the current storage times of quantum memories.

Alice measures  $\mu$ , so is able to estimate the maximum amount of information Eve gets from her photon number splitting attack. Eve's information can then be reduced to nothing in the privacy amplification step. Unfortunately this leads to poor performance in QKD systems. As the channel distance increases, Alice must decrease her photon number to stop Eve's attack because there will be added channel loss for Eve to hide her attack. This gives a quadratic dependence of the secure key rate on channel distance, because the channel loss is increasing at the same time as Alice's mean photon number is decreasing. Looking

again at Fig. 1.3, it is obvious that the probability of emitting multiple photons can be made vanishingly small by reducing the mean photon number, although this will also lead to a large probability of simply emitting no photons. When  $\mu=0.5$ , the ratio of multi-photon states to single photon states is 1 in 3.36 states, whereas when  $\mu=0.1$ , the ratio is just 1 in 19.34 states.

This solution is not perfect, however, because it means that no photons are being sent most of the time, which is inefficient. Decoy states are a useful solution to this, and are described in detail in Chapter 5.

### 1.3.4 Phase modulation

Intensity, polarisation and phase are three common light properties that can be controlled to transmit information. Sending polarisation-encoded signals in a fibre-optic system is challenging because perturbations in the fibre change the phase and polarisation unpredictably [60]. Continuous alignment is therefore required to ensure Bob's measurement bases align with Alice's preparation bases. For this reason, polarisation coding is predominantly used in free-space applications, rather than in fibre-optic applications, where the polarisation changes are much lower [49]. Phase coding, however, uses the relative phase between two close pulses to encode information. This means that regardless of changes in the fibre, both pulses experience the same phase change throughout [31].

The simplest method of phase modulation is direct laser modulation. Here, the current input to the laser diode is varied to change the output phase. Unfortunately, however, this simultaneously changes the intensity, wavelength and phase of the output light. This change of wavelength is undesirable in classical communications because it causes intersymbol interference as different spectral components of the light travel at different velocities in the fibre due to dispersion. This will reduce the signal-to-noise ratio of such systems. In QKD, the impact is even more heinous, opening a side channel for Eve to attack. A side channel is a flaw in the implementation of a cryptographic protocol that leads to an eavesdropper obtaining information. A simple example is if the transmitter were to audibly click every time a '0' bit is transmitted. Extended to direct phase modulation, an eavesdropper could measure the wavelength of each pulse, leaving the phase untouched and thus obtaining full information of the key without introducing any errors. For these reasons, an external modulator is most often used for phase modulation. Half-wave voltage (written as  $V_\pi$ ), is a metric to compare phase modulators and quantifies the voltage required by the modulator to achieve a  $\pi$  phase shift [61].

Phase modulators utilising the electro-optic effect are commonly used in practice. Materials are used that have a refractive index change in response to an external voltage. Devices based on Lithium Niobate ( $\text{LiNbO}_3$ ) are the most popular in QKD systems because they are easy to fabricate, have a good bandwidth and operate at achievable voltages [62].  $\text{LiNbO}_3$  crystals are highly nonlinear, birefringent and have a large electro-optic coefficient [63]. These properties mean that applying a voltage to the device creates an electric field that changes the material properties in an identifiable way. Light passing through the device experiences a phase shift

$$\Delta\phi = \frac{2\pi}{\lambda}\Delta n(V)L, \quad (1.7)$$

where  $\lambda$  is the wavelength of light,  $\Delta n(V)$  is the change in refractive index caused by an applied voltage  $V$  and  $L$  is the interaction length. This allows a voltage to modulate the phase of light passing through the device. Light makes a single pass through these modulators, hence  $L$  is simply the device length, which can lead to bulky modulators when low driving voltages are required.

In order to work at high rates, the architecture of electro-optic phase modulators must be modified in some way. If, for example, the device length is 10 cm, the pulse will travel through the material for roughly 770 ps, making the maximum speed of the device around 1.3 GHz. This is not fast enough for many practical applications, hence the electrodes are modified to ensure radio frequency (RF) signals travel through the device at the same speed as the light pulses. These devices are known as travelling wave modulators and can operate up to 40 GHz.

The half-wave voltages of  $\text{LiNbO}_3$  phase modulators is around 4-6 V, which often necessitates the use of RF electrical amplifiers [64], increasing the system complexity. It would make sense to increase the device length to decrease the half-wave voltage, however they are already of the order of 10 cm when packaged and impedance matching issues will occur if the length is increased. Another problem with these devices with regard to QKD is their loss, which is 0.2 dB/cm in the best case scenario [65]. Consequently, if the device is on one arm of an interferometer, as is the case for a BB84 transmitter, the other arm must be attenuated to create equal losses along each arm.

Organic electro-optic materials show promise for small footprint, low voltage and high bandwidth phase modulators [66]. When functioning, they are a better alternative to  $\text{LiNbO}_3$ , however they suffer from thermal and photochemical effects [67]. Accordingly, they are unreliable unless carefully packaged. This is a difficult process that increases the device size. Another issue is that it is challenging to grow the organic materials with high optical

quality [68]. LiNbO<sub>3</sub> devices are thus favourable for practical applications, and are found in many QKD systems.

### 1.3.5 Phase demodulation

The phase difference between light pulses is not a directly measurable property, so this information must be retrieved indirectly. This is possible by sending a pair of light pulses with a phase shift  $\Delta\phi$  through an asymmetric Mach-Zehnder interferometer (AMZI) with a variable phase delay on one arm. In this device, the light pulses are split equally into a fast and a slow path. The phase of the pulse in the fast path is modified in a controllable manner, whilst the pulse in the slow path is delayed by an amount equal to the separation between pulses.

There are two output ports from the AMZI, with light pulses in three separate time bins. The first (third) time bin comes from the first (second) incident light pulse travelling through the fast (slow) AMZI path. The middle time bin is the useful one, and is caused by the first pulse travelling through the slow path and the second pulse travelling through the fast path and then interfering at the output. This means the exit port of the middle time bin is defined by the phase difference between these pulses, which is  $\Delta\phi$  added to the phase shift incurred by the pulses as they travel in different paths. A train of coherent pulses can be made to all exit through the same port by tuning the phase delay on one path. The extinction ratio of light between the two exit ports can then be measured and used as a figure of merit for the phase coherence of the pulses.

A planar lightwave circuit (PLC) AMZI with a silica waveguide and a delay of 500 ps is used throughout this thesis. A fibre-based AMZI could also be used, however they are far more susceptible to changes in the ambient conditions, requiring complex tracking and compensation to stabilise. The entire silicon substrate on the PLC AMZI can be temperature controlled using thermoelectric cooling, meaning the device is resilient to ambient changes. A thermal phase shifter on one AMZI path tunes the phase delay between the paths. The main drawback of using the PLC AMZI compared to a fibre-based AMZI is the increased insertion loss. This is minimised by the use of a silica waveguide to match the optical fibre. At various points over the course of my PhD, the loss of this device was measured between 2 and 3 dB, depending on the experiment. This could be due to different couplers being used, or even due to the spectral properties of the light changing based on the experiment being carried out.

### 1.3.6 Phase randomisation

Randomness is the absence of predictability, meaning there is no pattern. It is a prerequisite for a number of parts in QKD systems. Firstly, for QKD to be secure, the key Alice prepares must be random. Secondly, Alice and Bob must randomly choose a separate encoding and measurement basis for each bit in BB84. Also, if discrete variable QKD is carried out using weak coherent pulses, the global phase of each signal should be random to maximise the secure key rate [69, 70, 71]. For example, in a phase-encoded implementation of BB84, the information is encoded between a reference pulse and a signal pulse, but the global phase of this pulse pair must be random.

To describe why this is the case, consider a laser emitting coherent states  $|\alpha\rangle$  with  $n$  photons, which can be defined as

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \quad (1.8)$$

Here,  $\alpha = \sqrt{\mu}e^{i\theta}$ , where  $\mu$  is the mean photon number and  $\theta$  is the phase. If the phase of the state is completely random and Eve has no knowledge of it, then the measurement result is indistinguishable from a Poissonian distributed mixture of photon number eigenstates:

$$|\alpha\rangle \langle \alpha| = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n\rangle \langle n|. \quad (1.9)$$

If the phase is not completely random then the state cannot be described in this way and thus Eve can obtain information from multi-photon pulses [71, 72].

### Randomness in practice

In many systems, pseudorandom number generators (PRNGs) are used to generate random numbers. These utilise an algorithm to create a set of random numbers from a seed state [73, 74]. A PRNG will always produce the same sequence from each seed state. Whilst this can be used to produce random numbers at a very high rate, they are not true random numbers, meaning the sequence will repeat after a certain number of bits. If a PRNG is used for a QKD system, the security is reduced because an eavesdropper who knows about the implementation of the number generation could theoretically exploit it [75, 76].

A true random number generator is necessary for QKD to ensure the security is not compromised. Quantum random number generators (QRNGs) are based on the fundamental randomness of physical processes [77] and provide us with the most obvious choice for QKD



systems. They have been proven to reliably produce perfectly random sequences at high speeds [78]. Recent work has shown the extraction of random numbers from a QRNG at a rate of 8 GBit/s continuously over 71 days, which is sufficient for QKD applications [79].

### 1.3.7 Finite-key-size analysis

Alice and Bob will perform QKD until they have built a raw key block of a certain size, say  $10^6$  bits. They will then perform post processing on this block. If they do this on many of these blocks, they will observe that the experimental parameters, i.e. the number of counts and the error rate, will have statistical fluctuations. This is known as the finite-key-size effect [69, 80, 81, 82, 83, 84, 85].

One way of dealing with these variations is to use the worst case scenario of the observed counts and error rate distribution. This involves assuming a normal distribution of the count rate and error counts, with a standard deviation defined by the block size. The tail end of these counts (usually lower for count rate and upper for error counts) can then be used in the secure key rate estimations. Better bounds can be placed on these fluctuations by taking advantage of various mathematical inequalities [86, 87].

According to the central limit theorem, the larger the block size used, the sharper these distributions will be. An asymptotic analysis is where no finite-key-size effects are accounted for, which would be the case for an infinitely large block. To this end, it is best to use the largest possible block sizes for post processing to reduce the statistical fluctuations.

### 1.3.8 Single photon detectors

SPDs are the most expensive and complex part of any DV or DPR QKD system. This is because they must be able to efficiently detect incident photons (or true positives), whilst ensuring they do not record a detection at any unintended times (or false positives). There have been significant advances to SPD technology that have allowed QKD to be demonstrated with reasonable secure key rates. The performance of SPDs can be characterised by a number of figure of merits [88]:

- Efficiency,  $\eta$ , is the probability of the detector registering a click given an incident photon. It is vitally important that this parameter is high due to the small mean photon number transmitted by Alice and the photon loss in the channel.
- Dark count rate is the number of detections per second given no light input. This is a difficult parameter to control, often requiring cooling the detectors and fibre near

the detectors to limit thermal photons. Other techniques such as wavelength filtering and polarisers can be used to reduce the dark count rate. These counts can be the limiting factor for producing a secure key at long distances when they are produced at a comparable level to those sent by Alice.

- Dead-time is the time after registering an event that the detector cannot operate. This can be the limiting factor for the maximum count rate the detectors can handle.
- Timing jitter is the uncertainty in the registered measurement time of an incident photon. High jitter values cause intersymbol interference, increasing the QBER.

Three single photon detector technologies are outlined in this section: single photon avalanche photodiodes (SPADs), transition edge sensor (TES) SPDs and superconducting nanowire SPDs (SNSPDs). The first can be operated at room temperature, whereas the latter two both require supercooling. State of the art results for all three detector types are outlined in Table 1.2.

### Single photon avalanche photodiodes

SPADs are the same in design as ordinary avalanche photodiodes (APDs). In APDs, a p-n junction is operated with a large reverse bias and incident light creates electron-hole pairs. The high bias causes them to accelerate towards the electrodes, ionising other carriers in the multiplication layer due to their energy. All of these ionised carriers travel towards the electrodes, creating a higher current than ordinary photodiodes. SPADs use a much higher reverse bias to ordinary APDs, giving them a higher sensitivity. InGaAs is commonly used as the active material for these detectors due to its band gap around telecommunication wavelengths.

SPADs are typically biased below their breakdown voltage, relying on a short pulse of large reverse bias at the same time as incident photons to act as a ‘gate’ to detect the photon. This is known as ‘gated mode’, however it incurs a large amount of noise from spurious avalanches due to carriers that have been trapped by defects [89]. This limits the gating frequency. Yuan et al [89] developed a method known as ‘self-differencing’ to reduce the noise, allowing a higher count rate to be achieved. This technique splits the electrical response from the detector into two, delays one and then subtracts it from the other, removing the capacitive response from the signal.

Afterpulsing is a negative effect seen in SPADs where a single photon event will create multiple detection events. This is due to avalanche carriers becoming trapped in deep levels of

the semiconductor band structure, causing a delayed response. It can cause an overestimation of the count rate of up to 10 % [90], and increases the measured QBER.

SPADs tend to have a lower efficiency and higher dark count rate than other SPDs, however even with these properties and afterpulsing, they are commonly used in QKD systems. This is because they are reliable, compact, cost-effective and can be operated at room temperature.

### **Transition edge sensors**

TES SPDs measure the resistance change as a photon incident on a thin layer of superconducting material causes the material to transition between its superconducting and conducting state. [88]. These detectors can be highly efficient with a low dark count rate. Unfortunately, however, their maximum count rate is low, they have to be operated as mK temperatures, and they have a slow response time. The main property prohibiting their usage in QKD systems is their large timing jitter, which can be up to 100 ns, making the maximum clock rate far lower than in other detection systems [88].

### **Superconducting nanowire single photon detectors**

SNSPDs are another popular choice for QKD experiments. These have a nanowire patterned on a substrate, which is cooled to a level such that the material is in a superconducting state [91]. The device is then biased close to its critical current. This current means that incident photons create a hotspot in the material, creating a change in the resistance and thus a measurable voltage pulse with a high time resolution.

The nanowire can be patterned such that the effective collection area is large, giving the detectors very high efficiencies. The low temperatures (around 4 K) also ensure the dark count rates are low, but also means the devices are expensive to operate. This being said, the temperature is not quite as low as in TESs, meaning closed-cycle cooling technology can be used [91]. Also, the material reverts to its initial state rapidly after the voltage pulse, giving low deadtimes.

SNSPDs are used for all protocols demonstrated in this thesis. They are characterised before each experiment, with their efficiency varying between 34-38 % and their dark count rate between 10-30 Hz, depending on the experiment. They have a maximum count rate around 38 MHz, however the timing jitter dramatically increases at count rates above 10 MHz, making them unsuitable for QKD at high count rates.

Table 1.2 **State of the art SPDs** at 1550 nm. TES: transition edge sensor; SD-SPAD: self-differenced SPAD.

Detector type	Efficiency (%)	DCR (Hz)	Max. count rate (MHz)	Temp (K)
SNSPD [92]	93	1	25	0.8
SNSPD [93]	0.4	0.001	–	0.4
TES [94]	89	400	0.05	0.11
TES [95]	95	–	1	0.1
SD-SPAD [96]	45	94000	500	293
SD-SPAD [96]	10	480	500	243
Gated-SPAD [97]	9.6	200	20	183
Gated-SPAD [98]	10	875	125	228

### 1.3.9 Current state-of-the-art and future potential

The highest secure key rate achieved comes from Yuan *et al.*, who demonstrate 13.7 Mbit/s with continuous operation over 4.4 days and a 2 dB channel [99]. This is made possible by using detector electronics with a high saturation rate that can process raw counts at fast speeds, removing bottlenecks with sifting, error correction and privacy amplification. In 2015, the longest distance for two-party QKD over optical fibre was demonstrated at 307 km [86]. This is achieved using detectors with a low dark count rate (0.9 Hz) and ultra low-loss optical fibres (0.16 dB/km), however the COW protocol is used, which does not have security against coherent attacks. Very recently, however, this record has been broken. Boaron *et al.* use ultra low-loss fibres, with even lower dark count rate detectors (0.1 Hz) and a clock rate of 2.5 GHz, to demonstrate QKD with security against coherent attacks over 421 km of optical fibre [100]. Previously, the record distance for the same protocol was 240 km [101], although it should be noted that this demonstration does not use cryogenic detectors. MDI-QKD has also been demonstrated over a distance of 404 km ultra low-loss optical fibre and 311 km of standard optical fibre [102].

Multi-user QKD networks are certain to be important in proving the practicality and enabling broader uptake of the technology. This would allow many users to be connected

with secure links. To this end, many networks have been implemented around the world, for example in America [103], Austria [104], South Africa [105], Switzerland [106], Japan [107], China [108] and England [109]. Some of these have indeed been used to transfer sensitive data between nodes. Swissquantum operated their QKD network for two years between three separate nodes in Geneva, whilst the network in Tokyo allowed secure TV conferencing over a distance of 45 km with help from nine organisations

Satellite QKD has seen a huge development in the past few years [52]. A landmark experimental demonstration by Liao *et al.* in 2017 demonstrated kilobit per second secure key rates over a distance of 1200 km using the Micius satellite [110]. As mentioned in Section 1.3.2, these enormous distances are reachable because of the negligible loss above the Earth's atmosphere. This experiment opens the door to secure communications over a global scale if users are willing to pay enough.

Low-cost and mobile QKD is also being explored in chip-based [111] and handheld systems [112, 113, 114]. Chip-based QKD is important for the wider uptake of the technology, allowing many components to be integrated together on a single device. This should bring down the cost of QKD components because it enables mass-production. The two technologies combined would allow for QKD to be implemented within mobile devices. This could demand docking stations to ensure the transmitter and receiver are aligned to maximise secure rates, making the application a little impractical.

One of the most recent advances in the field has come from the proposal of twin-field QKD (TF-QKD) by Lucamarini *et al* [115]. This protocol is similar to MDI-QKD, in that an untrusted third party is used, but uses first order interference from two transmitters instead of second order interference. This allows the secure key rate to scale with the square root of channel transmittance, enabling secure QKD over a longer distance than even decoy-state QKD. The protocol has generated a lot of discussion and activity in the field because of its potential [116, 117, 118, 119]. With current technology, TF-QKD would enable secure keys to be generated over the entire length of England.

## 1.4 Motivation for research

A metropolitan quantum network with all users linked would require transmitters to have separate hardware for each protocol and clock rate adopted by the various receivers. The motivation behind this thesis is to develop a quantum transmitter that is able to adapt to a number of different weak coherent pulse based QKD protocols with no changes to the

hardware. This would greatly simplify future quantum networks. The transmitter would desirably be small, versatile and energy efficient.

## 1.5 Novel contributions

This thesis develops a directly-modulated transmitter and applies it to QKD. The author has made the following novel contributions:

- Phase modulation has been shown using an optically injection locked system with a half-wave voltage of 0.35 V applied to laser diodes with a 50  $\Omega$  bias tee. This is the lowest recorded half-wave voltage for a phase modulator and has been shown at a clock rate of 2 GHz. The injection locking also has the benefit of reducing the pulse jitter.
- On-demand phase randomisation has been achieved using this system. Any pulse in a pattern can be given a random phase by driving the phase preparation laser below its lasing threshold. This is a requirement in a number of QKD protocols, and ordinarily either requires an unstable asymmetric Mach-Zehnder configuration in the transmitter or a random number generator and phase modulator. The randomness was tested by looking at the distribution of values and the autocorrelation functions.
- Three phase modulated QKD protocols have been demonstrated. The differential phase shift protocol has been implemented with a QBER of 1.70 %. The BB84 protocol has also been implemented, with a QBER of 2.03 %, along with the first ever experimental demonstration of the differential quadrature phase shift protocol. This was shown to achieve 2.71 times the secure key rate of BB84.
- Accurate intensity modulation has been shown with the directly-modulated transmitter, whilst providing a coherent phase to the pulses. The coherent one way protocol has been implemented with high extinction ratio intensity modulation allowing a 0.20 % QBER, alongside visibilities of 97.5 %.
- Concurrent phase and intensity encoding has been demonstrated with decoy-state BB84. The directly-modulated transmitter showed the ability to produce vacuum states accurately, however was unable to directly produce the decoy states without side channels. A patterning-effect-free Sagnac intensity modulator was therefore developed in order to provide the decoy states, with the directly-modulated transmitter giving the signal and vacuum states. This experiment allowed the first direct comparison between

polar BB84, which uses intensity and phase encoding, and phase-encoded BB84. This showed a 1.60 times improvement when using polar BB84, although it requires an extra intensity modulator to equalise the number of photons in each basis.

## 1.6 Organisation of thesis

This thesis is organised such that properties of the directly-modulated transmitter are explored and then applied to various QKD protocols. Chapter 1 gives a general introduction to cryptography and QKD. Different QKD protocols, how practical QKD has developed and also single photon detector technologies are detailed. Chapter 2 introduces the directly phase-modulated transmitter, describing how it works and characterising the spectra, visibility, half-wave voltage and the potential to provide on-demand phase randomisation. Chapter 3 details how the transmitter can be used to implement three different phase-encoded QKD protocols: differential phase shift, BB84 and differential quadrature phase shift. Chapter 4 looks at time-bin encoding, specifically showing intensity modulation by patterning the slave laser. The coherent one way protocol is implemented. Chapter 5 combines the properties explored in the previous two chapters, looking at concurrent phase and intensity modulation. Decoy-state BB84 is implemented with the X-Z bases and the X-Y bases for comparison. A stable two-level low extinction ratio intensity modulator based on a Sagnac interferometer is developed in this chapter to enable production of the decoy states with no side channels.





## Chapter 2

# A directly-modulated quantum light source

### 2.1 Introduction

In this section the operating principles of a directly-modulated transmitter that can be used for weak coherent pulse based QKD protocols will be outlined. The transmitter turns out to have many advantages over standard QKD transmitters.

#### 2.1.1 Laser diodes

Lasers are light sources that can produce highly monochromatic, coherent and collimated light beams [120, pp. 33–45]. Within a laser there is a gain medium surrounded by reflective mirrors, forming an optical cavity to confine photons. There are three processes involving light inside this gain medium, as shown in Fig. 2.1a. For ease of explanation, it is assumed the gain medium has two energy levels,  $E_1$  and  $E_2$ , where  $\Delta E = E_2 - E_1$ . The first process is absorption, which is where a photon of energy  $\Delta E$  is absorbed by an electron, exciting the electron from the lower to the higher energy level. The second is spontaneous emission, which is the random decay of an electron from the higher energy level to a lower energy level, producing a photon with energy  $\Delta E$ , a random phase and travelling in a random spatial direction. This decay has a characteristic time constant according to the material. The third process is stimulated emission. Stimulated emission is where an incoming photon with energy  $\Delta E$  causes the transition of a photon in the upper level to decay to the lower level. This produces two coherent photons, travelling in the same direction, with the same energy.

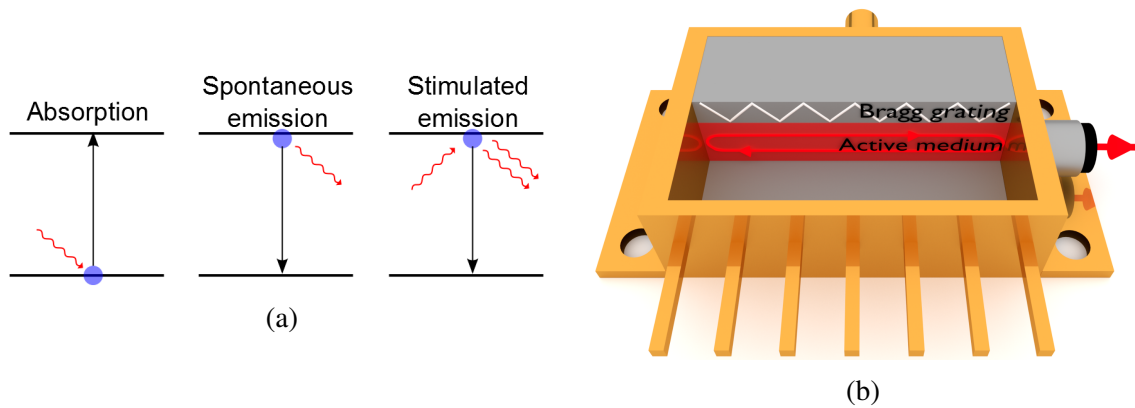


Fig. 2.1 **Laser fundamentals.** *a) The three processes involving light in a laser gain medium. b) The inside of a DFB laser diode, where a periodic grating above the active medium only allows certain wavelengths to oscillate. Laser light exits through the port on the right.*

The device is said to be lasing when the gain overcomes the losses in the cavity. These losses are caused by output coupling from the reflective mirrors, along with undesirable features such as absorption in optical components and scattering. The gain is the amplification of light inside the cavity and is proportional to the population inversion density (the difference in carriers in the upper and lower energy levels per metre cubed). When population inversion is achieved, stimulated emission can amplify the light in the gain medium, which oscillates between the reflective mirrors and creates further amplification. One of the mirrors has a slightly lower reflectivity, allowing a coherent light beam to be transmitted from the cavity. The exact method of achieving population inversion depends on the gain medium, but always requires some form of external energy injection to ‘pump’ carriers in the gain medium to a higher level.

The properties of the output laser light are highly dependent on the physical design of the laser. The gain medium, for example can be a gas, chemical, doped fibre, semiconductor, amongst other materials. This can change the output wavelength, power and mode of operation.

Semiconductor lasers are the most popular type of laser for telecommunications [120, pp. 48–71]. These use direct band-gap semiconductor materials with an active layer in between p-type and n-type layers. They are commonly electrically pumped using a strong forward bias, with electrons (holes) injected into the n-region (p-region) to create population inversion. Recombination of electrons and holes in the i-region creates photons. Their popularity in telecommunications is because they can emit efficiently at fibre-optic wavelengths (1310 nm and 1550 nm), they are small, easy to produce and package, can output milliwatt

powers, they can often be driven at GHz speeds, and they have a long lifetime. Also, the refractive index can be varied by changing the temperature of the diode, which shifts the cavity resonance wavelength. This gives a simple method of tuning the emission wavelength.

Semiconductor distributed feedback lasers (DFB) (see Fig. 2.1b) are a type of laser that is commonly used in optical communications [121]. This is because they have high modulation bandwidths, narrow spectral linewidths and are stable. These features are particularly useful in high-speed dense wavelength division multiplexing systems, where the wavelength should not overlap into neighbouring channels. The laser contains some form of patterned one-dimensional structure that acts as a Bragg reflector, reflecting a small range of wavelengths for amplification. This ensures the output light is in a single longitudinal mode and is highly monochromatic.

### 2.1.2 Optical injection locking

Injection locking is where two oscillators with similar frequencies adopt the same frequency and phase. The phenomenon was first discovered by Christian Huygens when he noticed that two pendulum clocks oscillate in phase with one another when close together on a common surface, but not when far apart [122]. This was found to be due to small vibrations caused by the clocks that induced a coupling between the two oscillators [123]. In the 1920s, it was discovered that the behaviour of an electrical oscillator could be modified by applying an external signal, in a manner similar to that found by Huygens. The differential equations defining this electrical injection locking were outlined in 1946 by Adler [124].

It is natural to extend this analysis to lasers, another form of oscillator. In this process, known as optical injection locking (OIL), light from a seed, or ‘master’, laser is sent into the cavity of an isolator-free ‘slave’ laser. The slave laser then emits light of the same frequency and phase as the seed laser. This is dependent on the frequency detuning,  $\Delta\nu$ , between the two free-running lasers being small, and sufficient power being injected into the slave laser. This occurs because external photons with an energy  $E_1$  close to the free-running energy of the slave cavity,  $E_2$ , act as the seed for stimulated emission at an energy  $E_1$ . This also means the emitted photons will have the same phase as the master laser photons. The process is described by a set of differential equations for  $S(t)$ , the slave laser photon number,  $N(t)$ , the slave laser carrier number and  $\phi(t)$  the difference between the phase of the slave and master lasers over time,  $t$ . These were outlined in 1982 by Lang [125, 126]:

$$\frac{dS(t)}{dt} = \{g[N(t) - N_{tr}] - \gamma_p\}S(t) + 2\kappa\sqrt{S_{inj}S(t)}\cos(\phi(t)), \quad (2.1)$$

$$\frac{dN(t)}{dt} = J(t) - \gamma_N N(t) - g[N(t) - N_{tr}]S(t), \quad (2.2)$$

$$\frac{d\phi(t)}{dt} = \frac{\alpha}{2} \{g[N(t) - N_{tr}] - \gamma_P\} - \kappa \sqrt{\frac{S_{inj}}{S(t)}} \sin(\phi(t)) - 2\pi\Delta\nu. \quad (2.3)$$

Here,  $g$  is the gain coefficient of the slave laser,  $N_{tr}$  is the carrier number at transparency,  $\gamma_P$  is the photon decay rate,  $\kappa$  is the coupling rate,  $S_{inj}$  is the number of injected photons,  $J(t)$  is the current injected to the slave laser,  $\gamma_N$  is the carrier recombination rate and  $\alpha$  is the linewidth enhancement factor of the laser. Whilst the specifics of these equations are not important in this thesis, it is important to note the coupling between the equations. The injected light field does not have a direct impact on the carrier density equation, however it does change the photon density, which then changes the carrier density. Also note that the two master laser parameters that can be tuned to change the output properties are injected power and frequency detuning.

### Benefits of optical injection locking

A number of favourable properties of optically injection locked systems have led to the technique being used extensively in classical optics.

Laser linewidth is the full width half-maximum of the laser spectrum. Finite linewidths can be caused by spontaneous emission of photons into resonant cavity modes, and also by the coupling between intensity and phase noise (defined by  $\alpha$  in Eq. 2.3) in semiconductor lasers. This coupling occurs because the refractive index of semiconductor lasers depends on the carrier density. OIL can reduce the slave laser linewidth to that of the master laser because the phase noise is inherited by the slave laser [127, 128]. The master laser can have a narrow linewidth because it can be driven far above its threshold where spontaneous emission is negligible. Narrow linewidths can be highly desirable in coherent optical communications [129]. This is due to the inverse dependence of temporal coherence on linewidth, meaning that a decrease in linewidth increases the coherence of the output, increasing the signal-to-noise ratio.

Semiconductor lasers experience relaxation oscillations due to the interplay between carrier density and photon density in the cavity. Applying a current pulse to the laser cavity injects a large number of carriers at a time where there are a low number of photons. This causes a large number of photons to be produced, reducing the number of carriers. This in turn causes a reduction in the photon number, and an increase in the carrier number. These two factors oscillate back and forth at a certain frequency until the steady-state condition

is reached, limiting the modulation speed of the system. OIL can improve this situation by using a large injection power and varying the frequency detuning to create a beating between the injected field and the slave laser cavity frequency, which then dominates the modulation dynamics and increases the resonant frequency (from a maximum of around 30 GHz to 100 GHz) [130, 131].

When directly modulating a laser diode, the carrier density inside the cavity is changed, which modifies the refractive index of the gain medium. This causes a time-varying change in the wavelength of the emitted light, which is equivalent to saying the laser is chirped. This can be caused by the laser relaxation oscillations when the laser reacts to sharp changes in the applied current. A chirped laser can have a broad range of wavelengths, meaning that chromatic dispersion will cause the symbols to temporally spread out in optical fibre, creating intersymbol interference at the receiver. This increases the bit error rate and thus limits the transmission rate. OIL minimises this chirp because the slave laser wavelength is locked to that of a continuous wave (CW) master laser, enhancing the possible transmission rate [127].

Relative intensity noise is the variation in the output power of a laser about its average power. This is caused predominantly by spontaneous emission. The slave cavity acts as a resonant amplifier to the injected master light, without adding any spontaneous emission. This means the output power is more stable than the original free-running output of the slave laser [132, 133].

Time jitter is where a pulse train does not have perfect periodicity, meaning pulses may arrive at different times within gates of a gated detector. This effect is prominent in gain switched lasers (described in the next section) because spontaneous emission is the dominant emission process for lasers below their lasing threshold. This means the carrier and photon density in the cavity is randomly fluctuating, hence will be at a random level at the start of each electrical pulse. Subsequently, the amount of time required to build up a positive gain resulting in a pulse will vary randomly [134, pp. 595–597]. OIL can be used to significantly reduce this jitter because the externally injected light helps to balance out fluctuations in the cavity [135].

Whilst the technique has been extensively used in classical communications, very limited research has gone into how it can improve quantum communications. Comandar et al [136] define ‘pulsed laser seeding’ for polarisation-encoded MDI-QKD. Here, both the master and slave laser are pulsed, but the master laser is above threshold for longer. By doing this, the output pulses can be locked to the steady state region of the master laser pulses, minimising the frequency chirp and time jitter, whilst ensuring the pulse phase is random and the pulse width is small. These conditions give a high quality second order interference between two

independent lasers and allow for the demonstration of the first megabit per second MDI-QKD system. In this thesis, OIL is primarily used for the phase inheritance, but the system is enhanced by the aforementioned properties that are beneficial in classical communications.

### 2.1.3 Pulse preparation

QKD deals with weak coherent pulses, thus the light source must be separated into pulses somehow. Fortunately, methods of pulse preparation have been well-researched because there are myriad uses for light pulses. For example, pulsed light can be used in telecommunications, for precise optical clocks [137] and even to study femtosecond chemical reactions [138].

In normal operation, the longitudinal modes in a laser oscillate independently. In a mode-locked laser, the phase relationship between all the longitudinal modes is constant, meaning they will periodically interfere with each other to create light pulses. The periodicity is proportional to the cavity length (and also, therefore, to the inverse of the spacing between lasing modes). Mode-locking can be active, for example where an intensity modulator is placed in the cavity to periodically modulate the cavity loss, or passive, for example where a saturable absorber is placed in the cavity. This process can be used to generate ultrashort and coherent light pulses, however the lasers can often be quite large, and the output can be unstable and noisy.

Gain switching is a more reliable method of pulse production than mode-locking, although it does create longer pulses with no phase relationship between one another [121]. Here, current is applied to a laser that is below its lasing threshold, and then quickly turned off when the laser is above its threshold. This happens because the injection of carriers into the laser cavity brings the device rapidly above the lasing threshold, generating many stimulated emission photons. This photon production depletes the laser cavity, at which point the current is turned off, thus stopping any subsequent emission. It is so-called due to the gain being briefly brought above the cavity losses, before rapidly being lower again. Gain-switching produces phase-randomised pulses because each pulse is stimulated from below threshold, which also explains why the pulses suffer from a high jitter. This loss of coherence can be beneficial in some QKD applications, as described in Section 2.2.6.

Pulses can also be produced externally by passing continuous wave laser light through a Mach-Zehnder modulator (MZM) or an electroabsorption modulator (EAM). MZMs split the light into two separate paths, with electro-optic phase modulators in each arm. Complementary phase shifts are applied to the light in each arm, giving precise control of the interference of the light as the paths are recombined at the output. EAMs utilise

semiconductors, which have an effective band gap energy that decreases with voltage. By using a material that has a band gap around the wavelength used, voltage changes can be used to control the output intensity of light. EAMs are attractive because they require far lower driving voltages than MZMs, however they only work over a small wavelength range, they often have a higher loss than MZMs and also a higher extinction ratio can only be achieved with a longer device, which can be prohibitive. External intensity modulators are desirable because they often have a higher modulation bandwidth than direct modulation and a lower chirp, although they increase the device complexity and cost. Using OIL does improve the characteristics of gain-switched lasers, however they are still not as good as external modulators.

Some QKD protocols require a phase-randomised pulse source, meaning gain-switching is the optimal solution. Other pulse-preparation methods would require extra components for phase randomisation. For QKD protocols that use a coherent phase, external modulators are often a better choice than mode locking due to their simplicity.

## 2.2 System design and properties

As QKD systems are commercialised, it is important that they are both compact and cheap. This means it would be highly favourable to use direct modulation in the transmitter rather than having to rely on external modulators. As pointed out in Section 1.3.4, side channels that could be exploited by an eavesdropper are easily introduced if care is not taken with direct modulation. Some modification is required, for example carving out the side channels with an intensity modulator, as shown by Hentschel *et al* [139]. Unfortunately, this still requires high-speed external modulation, it is simply performing a different task.

This section describes a quantum transmitter based entirely on the direct-modulation of two laser diodes. Optical injection locking of these lasers is exploited to remove the side channels that would ordinarily prohibit the use of direct modulation in QKD systems.

### 2.2.1 Transmitter design

The most important elements of the directly-modulated transmitter are two InGaAsP/InP multi-quantum well DFB laser diodes connected by a polarisation-maintaining circulator. Both lasers have a built-in bias tee, allowing an AC and DC to be simultaneously applied. They have a specified central wavelength of 1550 nm, a 1 MHz linewidth and a modulation bandwidth of 10 GHz. The circulator is a non-reciprocal passive device with three ports:

light entering port 1 exits through port 2 and light entering port 2 exits through port 3. The isolation for light in all other directions is specified as  $>50$  dB. The master laser is labelled as the ‘phase preparation’ laser and is placed at port 1 of the circulator. The slave laser is labelled as the ‘pulse preparation’ laser and is placed at port 2 of the circulator. The pulse preparation laser does not have an in-built isolator, thus light from the phase preparation laser is injected into the pulse preparation laser. Emission from the pulse preparation laser exits through port 3 of the circulator.

A schematic of the complete transmitter is shown in Fig. 2.2. The phase preparation laser is operated above threshold, so the light must be attenuated before injection into the pulse preparation laser. This is done using a non polarisation-maintaining digital attenuator. Both lasers have an output polarisation parallel to the slow axis, so injected light must also be in the same axis. To ensure this, and also to allow for a quick measurement of the injected power, an electric polarisation controller (EPC) aligns the light output from the attenuator into the slow axis of a polarising beamsplitter (PBS) by minimising the power into a power meter on the fast axis of the PBS. A polarisation-maintaining attenuator could be used to reduce the size and complexity of this system, however the described setup makes system measurements simpler while the system is being tested. A spectral filter is placed at port 3 of the attenuator to increase the quality of phase demodulation.

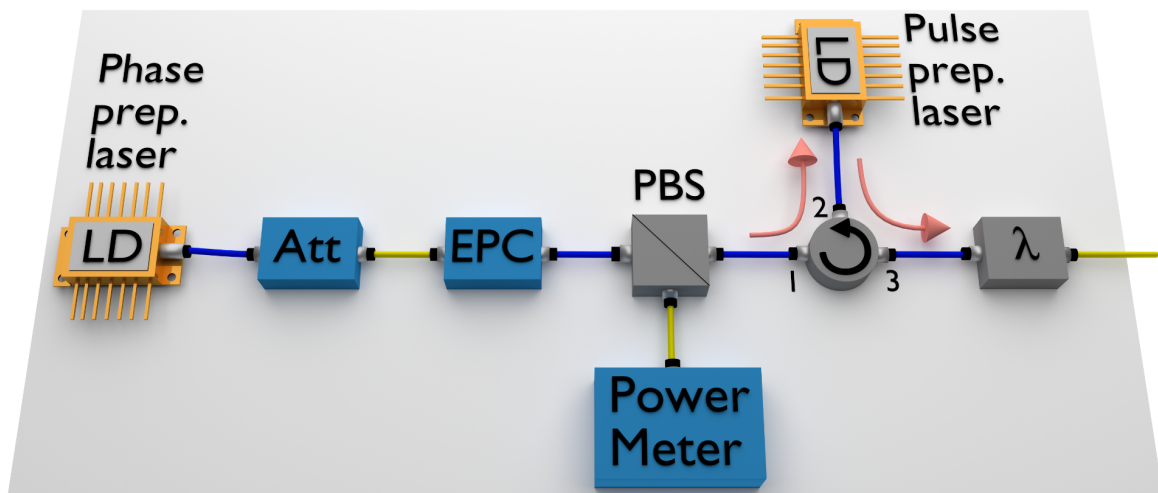


Fig. 2.2 **Experimental setup.** *Directly-phase modulated transmitter design.* LD=laser diode; Att=attenuator; EPC=electric polarisation controller; PBS=polarising beamsplitter;  $\lambda$ =wavelength filter. A circulator (with port numbers labelled) injects the light from the first LD into the second. Blue fibres are polarisation-maintaining, whereas yellow fibres are not.

The laser temperature is controlled using thermoelectric cooling. This is where a current is applied between two surfaces and the heat is transferred from one surface to the other by



the Peltier effect. This current is applied by a temperature controller with stability below  $0.002^{\circ}\text{C}$  and ensures the laser wavelength is insensitive to external temperature fluctuations.

### 2.2.2 Gain switched laser pulses

The pulses are produced by gain-switching, as described in Section 2.1.3. This creates very jittery pulses, as shown in Fig. 2.3 (top), with a high chirp and a random phase. Adding a spectral filter helps remove some noise, as shown by the second profile in Fig. 2.3, however the jitter can be further reduced by injecting a coherent laser, as shown by the bottom two traces. The pulse width is slightly broadened with the addition of the spectral filter because the pulse preparation laser temperature has to be varied to ensure maximum power output. The output pulse width is 61.5 ps with the 12 GHz spectral filter and the root mean square jitter is 2.20 ps. This is measured using a fast sampling scope with an optical bandwidth of 80 GHz and a sampling jitter of 425 fs. The small pulse width, combined with the low jitter, mean that the errors caused by a pulse entering the adjacent time bins will be minimal.

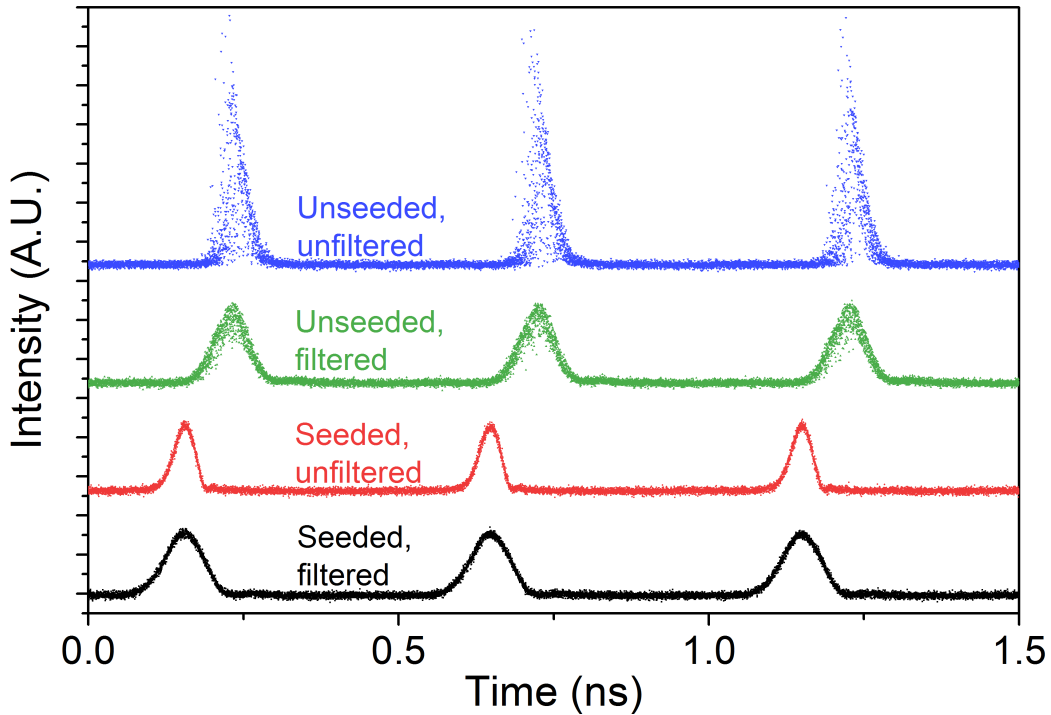


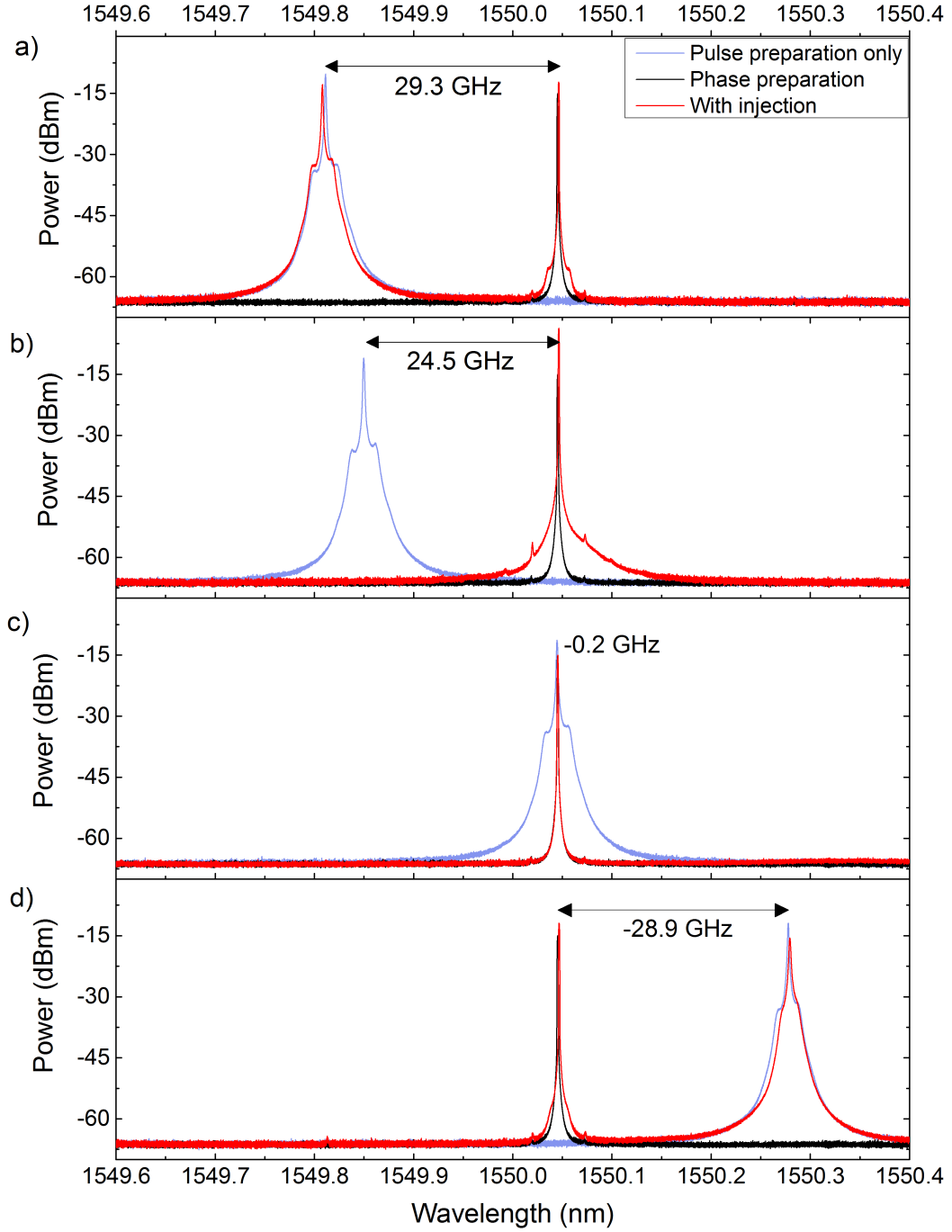
Fig. 2.3 **Gain-switched laser pulses.** Pulse profiles created by gain-switching the pulse preparation laser at 2 GHz. The DC bias is varied so the area under the pulses is similar with and without injection. The top two traces have no optical injection and are shown with and without a spectral filter. The bottom two traces have optical injection and are also shown with and without a spectral filter.

### 2.2.3 Spectra

The spectra of the various lasers are measured using a high-resolution (0.04 pm) optical spectrum analyser. The panels in Fig. 2.4 show the free running pulse preparation laser spectrum, the free running phase preparation laser spectrum, and the spectrum after injection. Free running in this situation means that the lasers are unmodulated and have no light injected into them. Identical laser diodes are used as the phase and pulse preparation lasers, however the figure shows that the linewidth of the phase preparation laser is narrower. This is because, whilst both lasers are driven above their lasing threshold, the phase preparation laser is driven further above threshold than the pulse preparation laser. This means it has a lower noise because it has a higher ratio of stimulated to spontaneous emission.

This figure also allows us to see how the laser responds to external injection at different detuning frequencies, where  $\Delta f$  is defined as the phase preparation laser frequency minus the pulse preparation laser frequency. Fig. 2.4a demonstrates the situation where the detuning is so large that the output with injection contains components of both the original wavelengths. As the detuning is reduced, the situation changes to that shown in Fig. 2.4b, where the output with injection is solely at the phase preparation laser wavelength, signifying that the system is locked. The weakness of this locking due to the large detuning is visible because the linewidth of the output with injection shows only a small enhancement over the free-running pulse preparation laser. When the detuning is just -0.2 GHz, as in Fig. 2.4c, the lasers are completely locked. The linewidth of the output is enhanced to match that of the phase preparation laser, and the emission is at the same wavelength as the phase preparation laser. At a negative detuning, shown in Fig. 2.4d, the same situation as for a similar positive detuning in Fig. 2.4a can be observed.

When the pulse preparation laser is gain-switched with DC below the lasing threshold, the output pulses have no phase relation, as shown by the ‘pulse preparation only’ curve in Fig. 2.5. Upon injection of external coherent laser light into the pulse preparation laser cavity, the output pulses inherit phase coherence. The result of this is an ‘optical frequency comb’, and can be seen in the ‘with injection’ curve in Fig. 2.5. This is created because the Fourier transform of an infinitely long train of perfectly spaced pulses at the same wavelength with a perfectly coherent phase is a set of equally spaced delta functions. The spacing of these delta functions is equal to the laser modulation frequency, which is 2 GHz in this demonstration.



**Fig. 2.4 Unmodulated laser spectra.** *Unfiltered spectra for free running phase preparation and pulse preparation laser diodes as the pulse preparation laser wavelength is varied to provide different detunings. All lasers have a DC bias above their lasing threshold. The phase preparation laser spectrum is measured after attenuation to 50  $\mu$ W. The detuning frequencies are 29.3 GHz, 24.5 GHz, -0.2 GHz and -28.9 GHz for panels a, b, c and d respectively.*

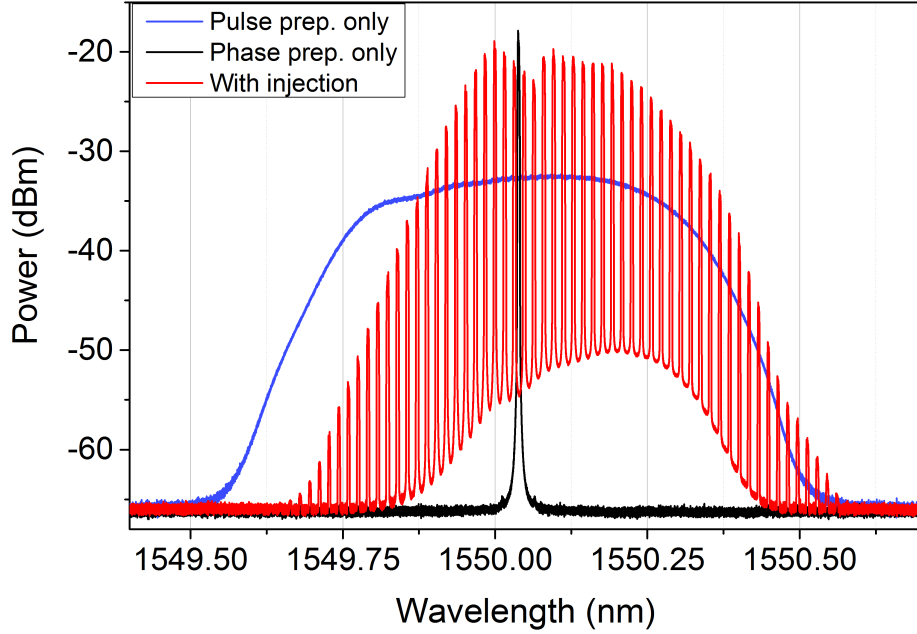


Fig. 2.5 **Gain-switched laser spectra.** *Unfiltered spectra for a gain-switched pulse preparation laser, with and without CW phase preparation laser injection (also shown). The AC voltage into the pulse preparation lasers is the same for both scenarios. The DC voltage is below threshold in both scenarios, however is higher without injection, to allow comparison in the plot.*

#### 2.2.4 Interference contrast and visibility

The output properties of the phase are of utmost importance for the system, so the quality of the phase inheritance from the phase preparation laser to the pulse preparation laser must be quantified. For this, an asymmetric Mach-Zehnder interferometer (AMZI) with a tuneable phase delay on one arm is used to interfere consecutive pulses. The power out of one arm of the AMZI is measured, noting the maximum and minimum ( $P_{\max}$  and  $P_{\min}$  respectively) as the phase delay is tuned about  $2\pi$ . This allows two important figures of merit to be determined, the interference contrast (in dB):

$$\text{Interference contrast} = 10 \log_{10} \frac{P_{\max}}{P_{\min}}, \quad (2.4)$$

and the visibility:

$$V = \frac{P_{\max} - P_{\min}}{P_{\max} + P_{\min}}. \quad (2.5)$$

Interference contrast is useful to visualise the phase inheritance, whereas visibility is directly linked to the QBER by the equation

$$\text{QBER} = \frac{P_{\min}}{P_{\min} + P_{\max}} = \frac{1 - V}{2}. \quad (2.6)$$

This can be visualised using Fig. 2.6, where any error photons exit from the wrong port of the interferometer.

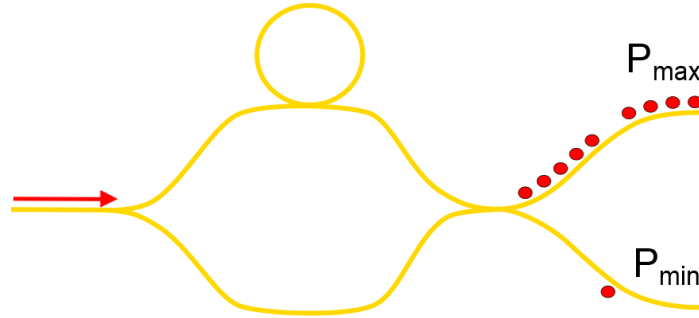


Fig. 2.6 **QBER origin.** An AMZI is aligned to measure in one basis. Photons exiting through the bottom port are contribute to the QBER.

In order to identify how the system responds to different phase preparation laser wavelengths, a high-resolution tuneable CW laser is injected into the pulse preparation laser. The power out of the pulse preparation laser as a function of injected wavelength allows the dominant lasing mode to be identified, along with any side modes. The interference contrast can also be used to identify where the peak phase inheritance occurs.

Fig. 2.7a shows that the maximum power output due to locking occurs at 1550.1 nm, aligning with the peak phase inheritance at 1550 nm shown in Fig 2.7b. The maximum interference contrast is 28.3 dB, which would correspond to an equivalent QBER of 0.15 %. The quoted DFB laser diode temperature tuning coefficient is -12.5 GHz/°C, which is equal to -100 pm/°C. The thermoelectric cooler used to control the laser diode temperature has a quoted stability of  $\pm 0.002$  °C, meaning the laser diode is stable to  $\pm 200$  fm. To increase the equivalent QBER to 0.20 % would require a wavelength change of 50 pm, 250 times higher than the laser stability, so it is extremely unlikely that ambient temperature changes will impact the locking strength.

The interference contrast measurements for both types of laser used are shown in Fig. 2.8, with a varied injection power. The pulses produced by a free-running gain-switched laser have an inherently random phase because the lasing is produced from spontaneous emission photons inside the cavity. This can be seen at low injection powers in Fig. 2.8 where the

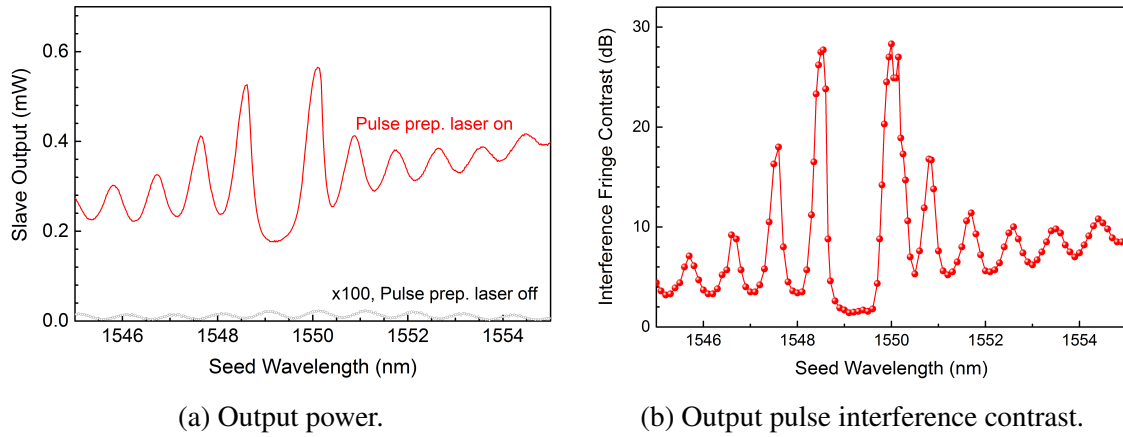


Fig. 2.7 **Master wavelength variation.** The pulse preparation laser is gain switched at 2 GHz and the output properties are measured as 50  $\mu$ W of CW light at different wavelengths is injected via a tuneable laser source.

interference contrast, and subsequently the visibility, are both zero. As the injection power increases, the output pulses inherit the phase coherence of the phase preparation laser. The tuneable laser has a narrower linewidth than the DFB laser diode. Laser coherence is inversely proportional to the linewidth, meaning that the tuneable laser has a longer coherence time, as is observed in the figure by a better interference contrast value. The coherence of the laser diode is still high, with a visibility over 99 %, which would give the very low QBER of 0.5 %.

### 2.2.5 Phase modulation

Phase modulation can be realised with this system by applying short modulation pulses, of size  $\Delta I$ , to the phase preparation laser, which is free running with a current  $I$ . A change in the phase preparation laser current to  $I + \Delta I$  will change the intensity, frequency and phase evolution of the light injected into the pulse preparation laser. A change in intensity or frequency depending on the desired phase shift will introduce a side channel that Eve can use to exploit the system. With this in mind, the modulation pulses must occur between two pulse preparation laser pulses, so that the current causing the gain switching is always  $I$ , thus preventing any changes in intensity or frequency. The size of  $\Delta I$  will determine the amount of phase modulation applied. This concept is shown in Fig. 2.9. The practical implementation is given in Fig. 2.10, with  $0, \pi/2, \pi, 3\pi/2$  modulations created by different modulation levels. The phase preparation laser remains above threshold at all times to ensure the coherence is not broken.

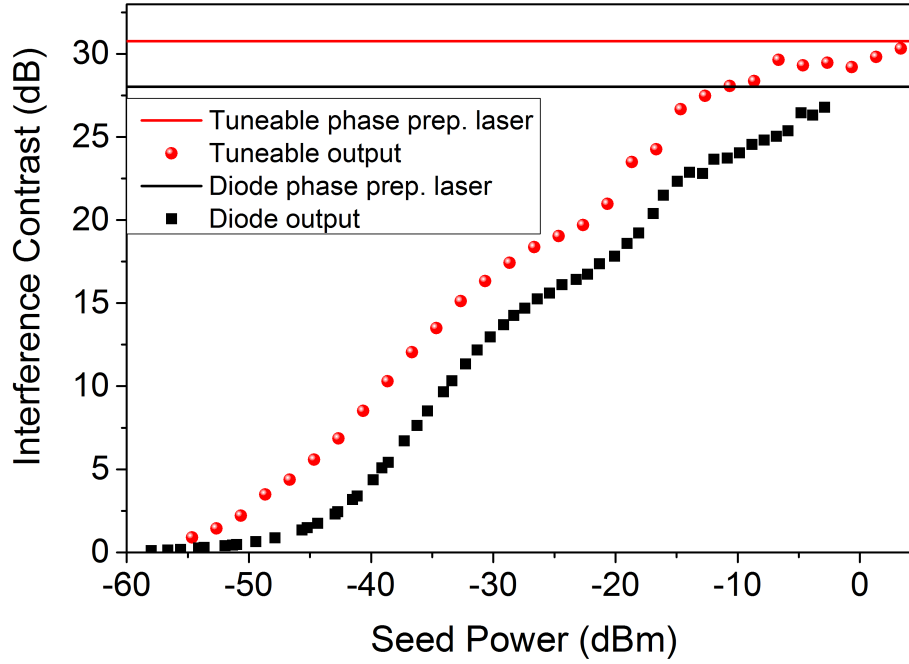


Fig. 2.8 **Interference contrast.** Evolution of the interference contrast with the injected seed power for a tuneable CW laser and a CW DFB laser diode. The pulse preparation laser is gain-switched at 2 GHz. Solid lines show the measured coherence of the phase preparation laser, whereas symbols show the system output with light injected into the pulse preparation laser.

One of the most important figures of merit for a phase modulator is the half-wave voltage. A repeated  $0-\Delta\phi$  pattern is input to the phase preparation laser and the 250 ps modulation depth is varied. The voltage is applied to the laser diode through a 50  $\Omega$  bias tee. The incurred phase shift is measured by tuning the AMZI phase delay and observing how the two modulation levels evolve with respect to one another. Fig. 2.11 shows that the directly phase-modulated transmitter has a half-wave voltage of 0.35 V. This is the lowest reported value for any phase modulation system, and is around 10 times lower than in  $\text{LiNbO}_3$  phase modulators (see Section 1.3.4).

This record-breaking half-wave voltage is made possible by the fundamental operating principles of the system. The modulation to the phase preparation laser changes the carrier density inside the cavity, which alters its refractive index, thus changing the phase shift experienced by the photons. The photons inside the cavity oscillate multiple times through this different refractive index, in contrast to a traditional phase modulator where the light only makes one pass. This is the cavity-enhanced electro-optic effect and ensures that although

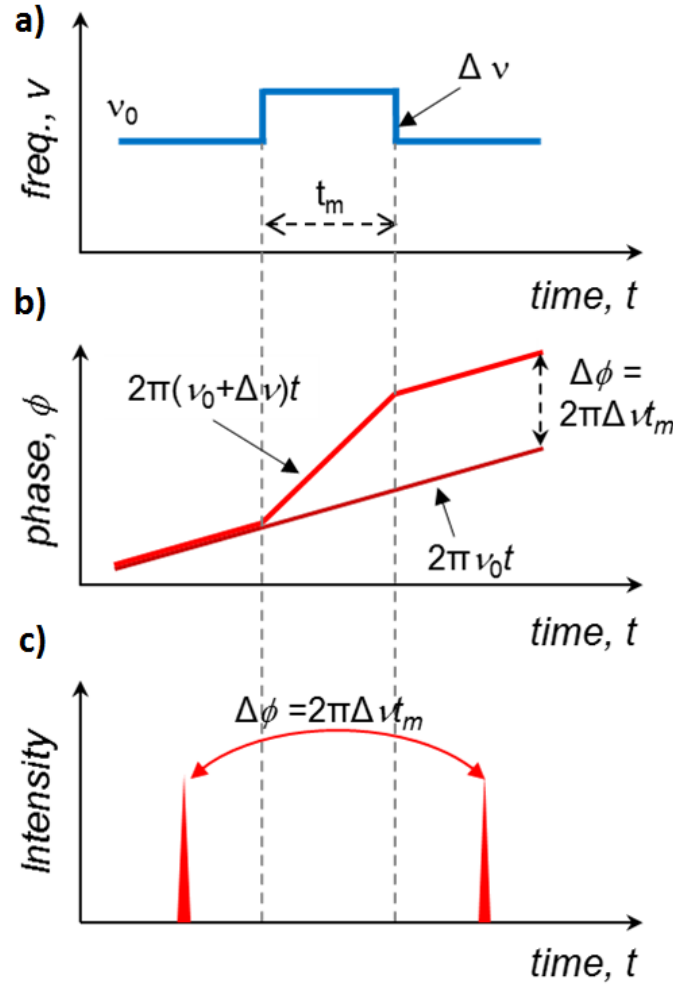


Fig. 2.9 **System concept.** a) The frequency change,  $\Delta\nu$ , caused by a perturbation of length  $t_m$  to the driving signal, alongside b) the change in phase,  $\Delta\phi$ , compared to the original phase without the perturbation and c) the subsequent output pulses, with a phase modulation, but no change to the intensity or frequency.

the device length is around  $100\ \mu\text{m}$ , the effective interaction distance is around  $25\ \text{mm}$  when the modulation time is  $250\ \text{ps}$ .

### 2.2.6 Practical phase randomisation

The directly-modulated transmitter removes the need for an extra phase randomisation step in QKD protocols utilising weak coherent pulses. This is possible by exploiting the fundamental physical properties of lasers. When a laser is emitting light above its lasing threshold, the light is generated mainly by stimulated emission, a process that generates photons with a



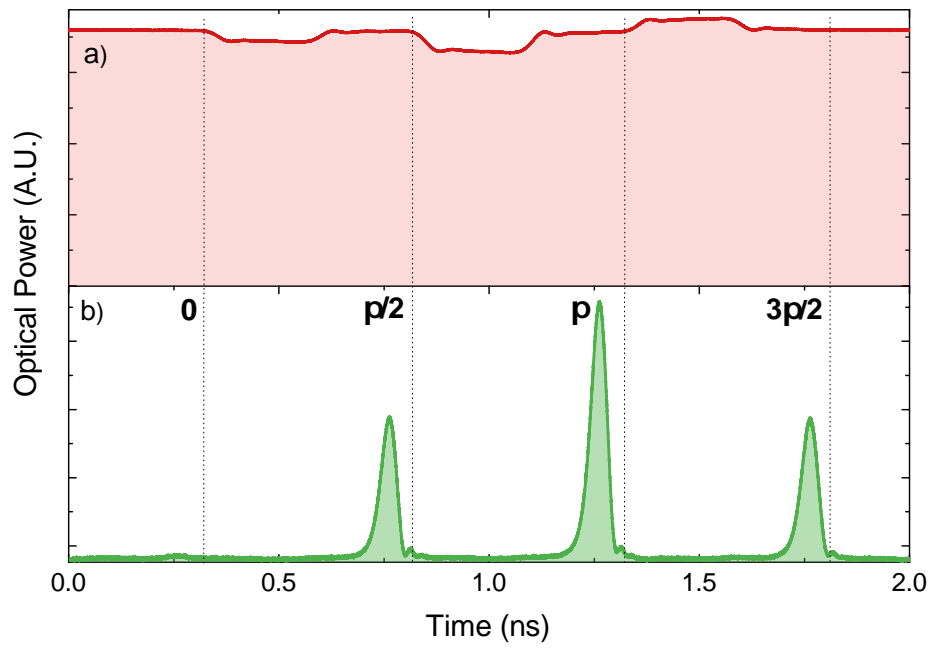


Fig. 2.10 **Phase modulation.** Shallow phase preparation laser modulations create arbitrary phase modulations in the system output measured using an oscilloscope. a) Optical response from the phase preparation laser; b) output from one arm of an AMZI.

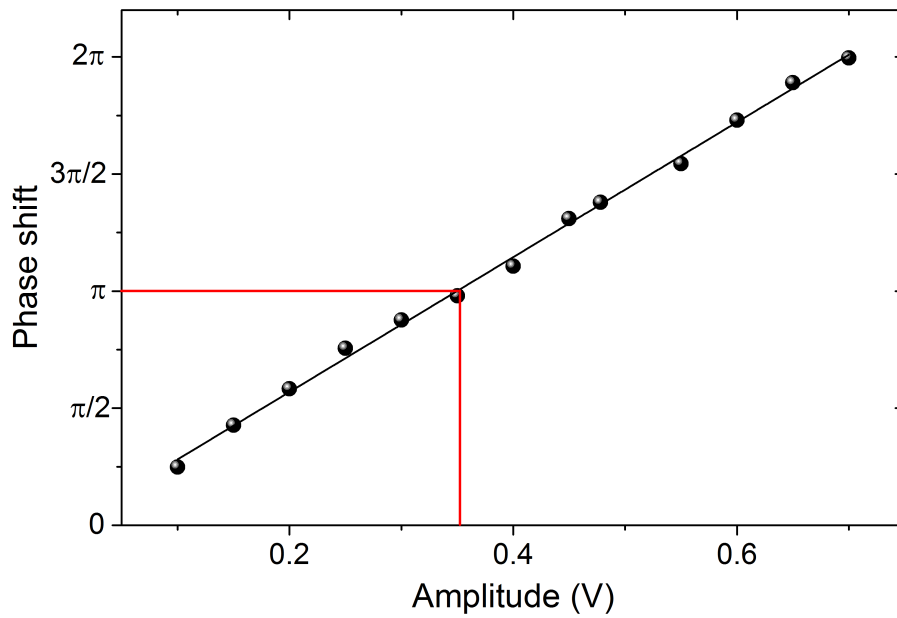
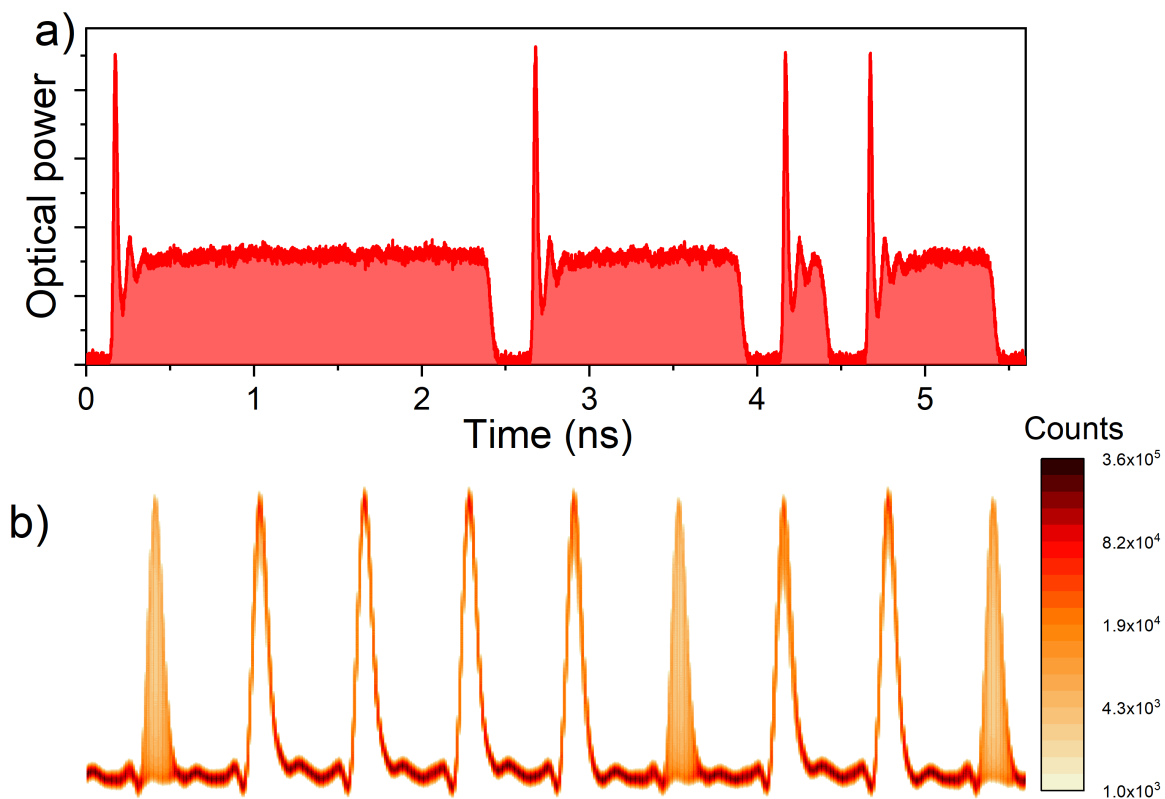


Fig. 2.11 **Half-wave voltage.** The phase shift between output pulses as a function of phase preparation laser modulation depth.

coherent phase. When the laser is emitting light below its lasing threshold, however, the system is dominated by spontaneous emission, a process with a completely random phase evolution [140].

The phase coherence of a laser above threshold can be broken, therefore, by driving the laser below threshold for long enough that spontaneous emission becomes dominant. When the laser is then driven above threshold, it will start lasing with a random phase due to lasing being seeded by a spontaneous emission photon. This can be seen when gain-switching a laser diode, where each pulse is produced with a completely random phase. This principle can be applied to the phase preparation laser before injection to the pulse preparation laser. Because the pulse preparation laser inherits the phase of the phase preparation laser, output pulses after a phase preparation laser modulation below threshold will have a globally random phase, as shown in Fig. 2.12.



**Fig. 2.12 Injection-locked phase randomness.** Phase randomness can be arbitrarily provided to pulses at 2 GHz by driving the phase preparation laser below threshold. a) Optical output from the phase preparation laser, showing depletion regions followed by peaks before a steady state region. The applied electrical signal has a down-time of 250 ps, whereas the optical down-time is around 200 ps. b) Colour-graded density plot of the output pulses after an AMZI.

### Randomness testing

There are a number of tests that can be run to determine whether a set of numbers is truly random [74]. A first basic test is to see if the data is uniformly distributed. This can be tested by looking at a histogram of the produced values. A second test is to ensure the data is independent, meaning there is no correlation between values. The independence of the dataset can be described quantitatively by measuring the autocorrelation function (ACF) of the data. This is the similarity of the dataset with respect to a delayed version of the same dataset. The ACF of a discrete dataset,  $a$ , is defined as the covariance of a dataset with a delayed version of itself divided by its variance:

$$\rho_x = \frac{\sum_{l=x+1}^L (a_l - \langle a \rangle)(a_{l-x} - \langle a \rangle)}{\sum_{l=1}^L (a_l - \langle a \rangle)^2} \quad (2.7)$$

where  $x$  is the delay, also known as the lag, and  $L$  is the string size. In the implementation in this thesis the data is normalised to have zero mean and unit variance, then the Matlab function 'xcorr' is used to extract the ACF.

Although it is usually obvious from the ACF plot if there are any correlations, the distribution across lags should also be tested, showing that there is no bias in the autocorrelations. The autocorrelations should have a normal distribution about zero for a random string, allowing confidence bounds to be determined for the probability of a point at each lag lying within a certain interval. Bounds,  $P$ , for a given confidence level,  $\alpha$ , and  $N$  samples, based on a normal distribution of autocorrelations about zero are found using the inverse error function [141]:

$$P = \sqrt{\frac{2}{N}} \times \text{InverseError}(\alpha). \quad (2.8)$$

The larger the sample used for the autocorrelation, the tighter the bounds will be, meaning a large sample should be used for more confidence in the result. Also, it should be noted that the ACF will always be unity at a lag of zero, because the correlation of a function with itself with no delay will be unity. For this reason, it is common practice to ignore the zero lag value in plots.

### Experimental Results

The experiments are carried out with a 2 GHz gain-switched pulse preparation laser and a phase preparation laser injection power around 50  $\mu\text{W}$ , with the phase preparation laser modulated to provide pulses with a phase alternating between random and coherent. A

negative applied voltage breaks the phase coherence of the phase preparation laser by emptying the laser cavity. The setup produces an output power around  $300 \mu\text{W}$  when there is no detuning between the two laser diodes. Measurement of the phase is performed using an AMZI with a one-bit time delay in one arm. This will produce an intensity,  $I$ , proportional to  $1 + \cos \Delta\phi$ , where  $\Delta\phi$  is the phase difference between consecutive pulses. Data is acquired from classical signals through a photodiode logged on an oscilloscope and analysed in Matlab.

In order to check the bulk data ‘looks’ random, the histogram of interference values for pulses on either side of a coherence-breaking phase preparation laser pulse is taken. The data is shown in Fig. 2.13. In a perfect system, the distribution would be symmetric, with narrow peaks at ‘0’ and ‘1’ because  $\Delta\phi$  should have a uniform distribution. This is not observed in practice however. In reality, both peaks are broadened, with broadening of the peak at ‘1’ being larger, meaning the height is less than that at ‘0’. To explain this, a simulation of the physical system is implemented in Matlab by creating a uniform random array with values between 0 and  $2\pi$  and then calculating  $1 + \cos \phi$  for each value. Two random variables from a normal distribution with a mean of zero are added to each array before calculating the expected distribution after interference. The first has a constant standard deviation, which accounts for the measurement uncertainty in the scope and any system fluctuations. The second has a standard deviation proportional to the interference intensity, which accounts for the linear intensity-dependent time-jitter of the pulses.

It is also useful to identify how long the laser needs to be below threshold to ensure the phase is randomised. The resolution of the AWG is 24 GSamples/s, so the down-time lengths are limited to multiples of 41.67 ps. The results for three different down-times are shown in Fig. 2.13. A down-time of 42 ps produces a distinct phase, as shown by the interference not spreading out over the entire phase range, meaning that there are many photons remaining in the laser cavity between pulses. The shape looks similar to what is expected with a down-time of 83 ps, however is biased towards lower intensities, meaning that there are still residual photons in the laser cavity. A down-time of 125 ps is sufficient to empty the phase preparation laser cavity and ensure the phase of the blocks is randomised. These experimental results fit well with the simulation for this down-time value.

The second step involves looking at the ACF of the produced data. These are shown in Fig. 2.14 for the inter-block interference in a BB84 pattern with  $10^6$  ‘0’ bits (ensuring no randomness is added from the pattern) and are aligned with what is expected for random data. There are no patterns in the ACF, and the values are distributed within the confidence bounds for the dataset. This further confirms that the phase of the blocks is globally random.

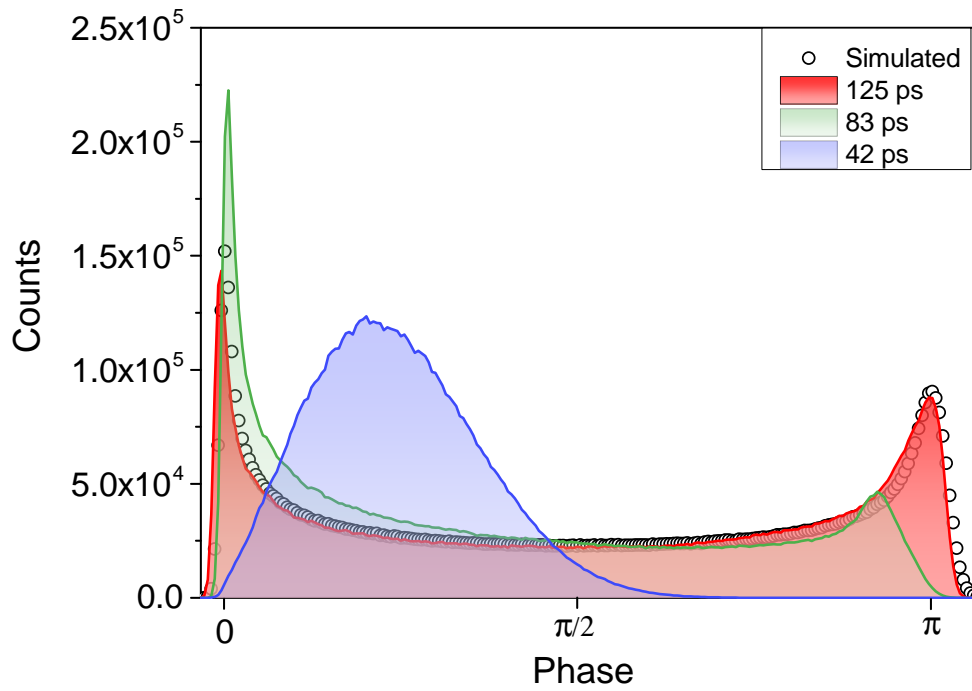


Fig. 2.13 **Randomness histogram.** Histograms of the random bits in a BB84 pattern for different down-times to break the phase coherence of the phase preparation laser. A simulation of the expected histogram is also given.

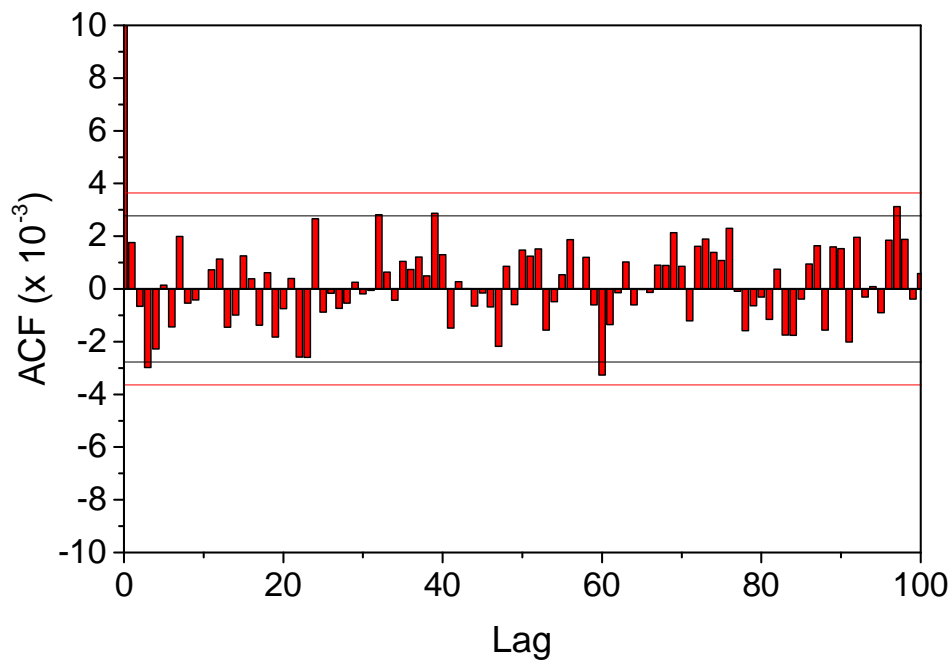


Fig. 2.14 **BB84 Autocorrelation.** Inter-block interference only. The outer lines (red) show 99 % confidence bounds and the inner (blue) lines show 95 % confidence bounds.

## 2.3 Summary

This chapter has outlined the optical injection locking of lasers and described some of its favourable properties. Also, different methods of phase modulation, demodulation, randomisation and laser pulse preparation are discussed. Bringing these ideas together, a directly phase-modulated transmitter system based on optical injection locking is introduced. Here, light is injected from a phase preparation laser into a 2 GHz gain-switched pulse preparation laser, producing pulses with the same phase as the injected laser. The phase coherence of the output pulses is measured through an interferometer with a one-bit delay. It is shown that 50  $\mu\text{W}$  of injected power from a CW DFB laser diode gives rise to a visibility equivalent to a QBER of 0.5 %. As well as giving coherent pulses, the injection locking is shown to drastically reduce the pulse jitter.

Next, the possibility for realising phase modulations to the output pulses is described by applying small modulations to the phase preparation laser between gain-switched pulse preparation laser pulses. The lowest reported half-wave voltage for a phase-modulation system, of 0.35 V, is achieved using this system. This is possible due to the cavity enhancement effect where light makes multiple passes through the laser cavity with a shifted refractive index.

Finally, the necessity for phase randomisation in QKD is explored. It is shown that the inherent randomness of lasers below their lasing threshold can be exploited in order to produce arbitrary phase randomisation. A histogram of the interference between two pulses with a random phase is analysed, and it is shown that a phase-preparation laser modulation below the lasing threshold for 125 ps ensures the following locked pulse-preparation laser pulse has a globally random phase. This result agrees with simulated data and the ACF of the produced data further confirms that true randomness has been achieved.

# Chapter 3

## Phase-modulated QKD

### 3.1 Introduction

As discussed in Chapter 1, there are a number of different QKD protocols that can be implemented with phase modulation. In this chapter different methods of phase encoding are introduced and three phase-encoded QKD protocols are demonstrated, each with different requirements on the transmitter.

### 3.2 Phase encoding

Phase encoding is an efficient method of encoding information on light that is commonly used in telecommunications, where it is called phase shift keying (PSK). PSK can be implemented in two main ways. The first method, coherent PSK, requires coherent detection, which is where the phase of a modulated signal is compared to that of a reference signal. This can be difficult because precise knowledge of the drifting channel phase is required in order to extract the modulated phase [142]. The second, known as differential PSK, is where the transmitted signal is referenced with respect to another signal. More clearly, this means that the phase shift of a signal is the difference between its phase and the phase of the previous signal. This creates a simpler system by removing complexity from the receiver, although it does introduce more errors than in ordinary PSK.

$M$  phase levels allow  $\log_2(M)$  bits of information to be encoded per symbol, meaning that more phase levels give a higher bandwidth efficiency. Commonly, two (binary PSK), four (quadrature PSK) or 8 (octal PSK) phase levels are used. Any higher than this leads to

diminishing returns because the signal-to-noise ratio will decrease as the points are closer to one another, increasing the bit error rate.

QKD requires qubits to be encoded as orthonormal states in conjugate bases. This means that there are two potential phase bases that can be used, with the same levels as in quadrature PSK. The X basis contains the phases 0 and  $\pi$ ; the Y basis contains the phases  $\frac{\pi}{2}$  and  $\frac{3\pi}{2}$ . Phase-based DV protocols require a differential phase encoding, meaning an interferometer must be used for demodulation, which often adds losses to the signal. This means that the receiver for polarisation encoded QKD can be less lossy (see Section 1.3.4), although phase encoding is far better for fibre optic applications due to the insensitivity to distortions in the quantum channel.

### 3.3 Distributed phase shift

The traditional differential phase shift (DPS) protocol [143] is a distributed phase reference (DPR) protocol and is one of the simplest QKD protocols to implement. A single basis is used to encode the data and to check for an eavesdropper. This is possible by maintaining a coherent phase amongst all pulses and then modulating the information on the differential phase between consecutive pulses. On average, each pulse contains less than one photon. Each photon spreads out over a number of time bins that depends on the temporal coherence ( $t_c$  of the source. The probability of a photon being phase coherent with another photon a time  $t_c$  away is  $1/e$  (37 %), meaning it is probable that they have no phase relation. The total wavefunction is therefore the tensor product of all individual time-bin photon states. Bob's measurements occur randomly among time bins and tell him the relative phase between a single pulse and the preceding pulse. This means that to conduct a successful attack, Eve would have to know Bob's measurement times in advance. If she makes a random guess at the measurement time, she will sometimes collapse the wavefunction at the wrong time and introduce errors in Bob's measurement.

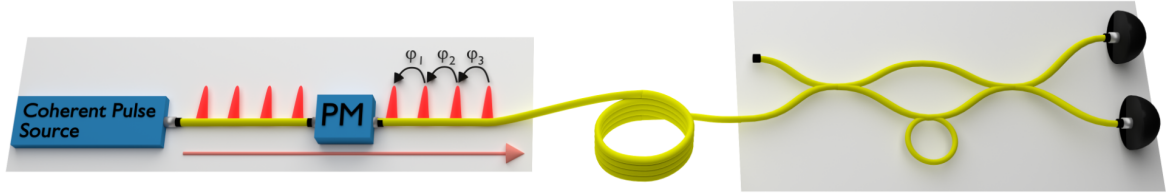
The main drawback of the DPS protocol is that it is insecure against coherent attacks. This is where Eve entangles a probe with the entire waveform and stores it in a quantum memory. When Bob announces his measurement times, Eve can then measure her probe in the same locations and obtain full knowledge of the key without introducing any errors.



### 3.3.1 Theory

A common implementation of the DPS protocol [144, 145, 146] is shown in Fig. 3.1 and the steps taken by Alice and Bob are:

1. Alice prepares a random string of bits to encode onto weak coherent pulses, where 0 indicates no phase modulation and 1 indicates a  $\pi$  phase modulation.
2. Alice attenuates her signal so the average photon number per pulse is around 0.2 and then transmits the photons through the quantum channel to Bob.
3. Bob uses a one-bit time delay interferometer to interfere consecutive pulses and measures the result using SPDs at both interferometer outputs. If his interferometer is aligned in the same basis as Alice's encoding basis, the SPD that clicks indicates the bit value. He records the time and value for each measurement.
4. Bob communicates his timing information to Alice, but not which detector clicked, allowing them to perform error estimation, error correction and privacy amplification.



**Fig. 3.1 Differential phase shift schematic.** One method of implementing the DPS protocol uses a coherent pulse source (for example a carved CW laser) and a phase modulator, PM, to encode the relative phase,  $\phi_i$ , between pulses. After travelling through the quantum channel, Bob's receiver is a passive interferometer measuring signals in a single basis.

Many DV protocols use two bases, leading to a sifting loss when the users choose mismatched bases. This loss is not present in the DPS protocol, meaning that all detected photons will give a raw key bit. Another advantage over DV protocols is that just two single photon detectors are required.

An upper bound of the secure key rate is given by [147]

$$R = -p_{\text{click}} \left[ (1 - 2\mu) \log_2 \left( 1 - E^2 - \frac{(1 - 6E)^2}{2} \right) + f(E)h(E) \right], \quad (3.1)$$

where  $p_{\text{click}}$  is the probability of Bob's detector clicking,  $\mu$  is the mean photon number per pulse,  $E$  is the QBER,  $f(E)$  is the efficiency of error correction and  $h(E)$  is the binary entropy function.

### 3.3.2 Directly-modulated implementation

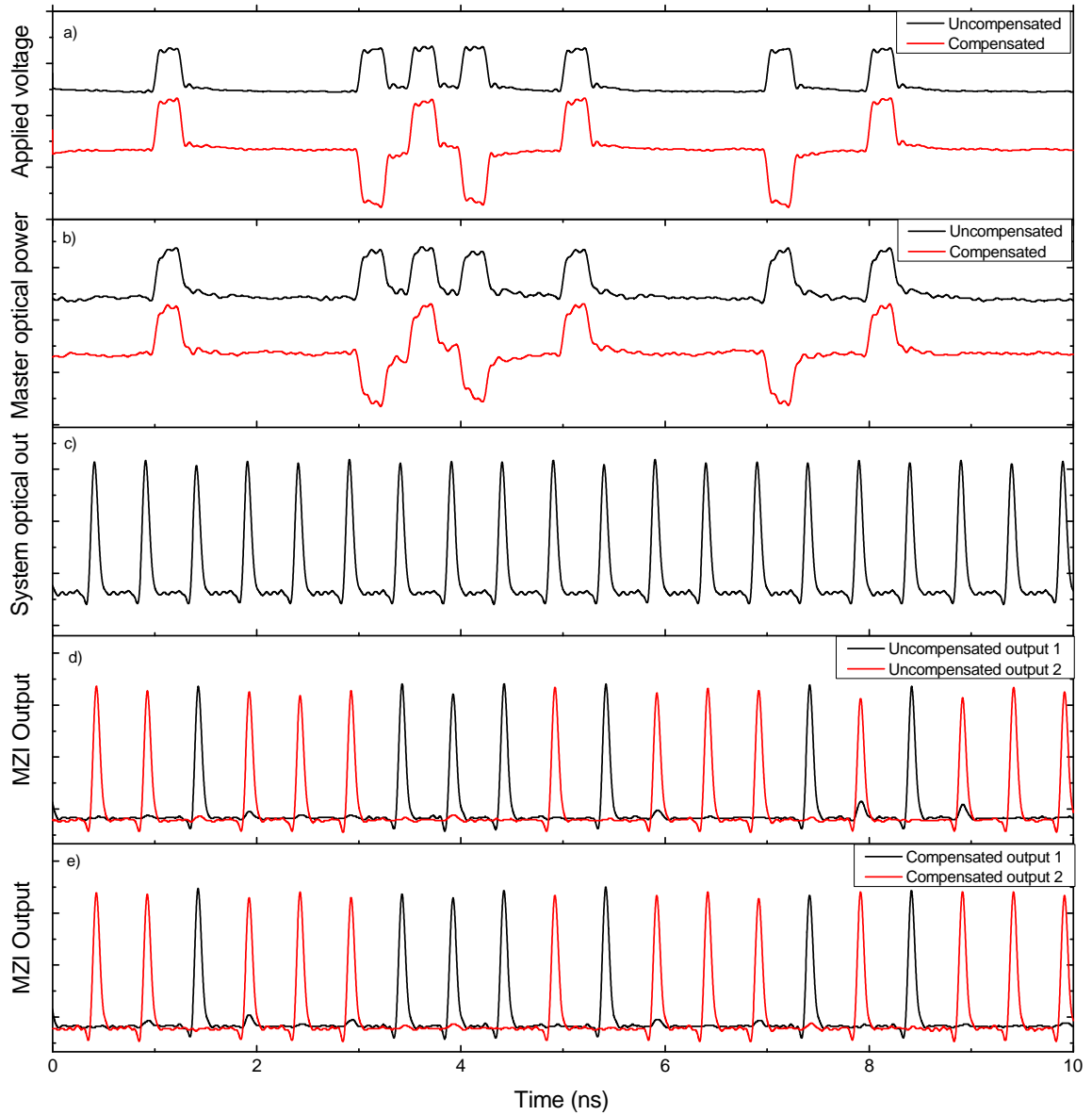
The DPS protocol is the simplest protocol to implement using direct modulation because it uses just a single basis and no phase randomness is required. The principle behind the phase modulation with no intensity or frequency modulation was described in Section 1.3.4. Modulations are applied to the phase preparation laser when a  $\pi$  phase shift is required, and the signal is kept constant when there is no phase shift. The phase preparation laser is driven with a high DC bias, meaning the visibility is high because the ratio of stimulated emission to spontaneous emission is also high. The pulse preparation laser is biased just under its lasing threshold and a 3.3 V AC square wave is applied to gain switch the laser. The phase preparation laser is injected into the pulse preparation laser via a circulator, transferring the high visibility to the output, giving phase-modulated pulses with a low QBER.

On the receiver side, a PLC AMZI with a time delay of 500 ps on one arm is used to interfere consecutive bits. A heater on one arm tunes the measurement basis and a temperature controller over the entire device ensures it remains stable. The stability of both the transmitter and receiver ensure that once a basis is set, it requires no stabilisation for the entire experimental period.

An example of the electrical pattern applied to the phase preparation laser and its subsequent output is shown in Figure 3.2a,b). The output after injection is given in Figure 3.2c), showing no variation in the output intensity due to the modulations. The AMZI output is given in Figures 3.2d,e), where the different colour corresponds to a different output arm, and therefore a different bit value.

The protocol was initially carried out using a binary electrical signal, with either a constant positive or negative  $\pi$  phase shift applied, as shown in the upper trace of Fig. 3.2a). In QKD systems Alice's pattern has to be completely random, meaning that a sequence of many repeated '0' bits, '1' bits or alternating '0-1' bits are equally likely. The mean DC value is completely different for each of these cases, which creates a problem because the phase shifts for the same modulation size changes throughout the pattern. This effect is observed in Fig. 3.3a, where a drop in the average DC of the pattern creates changes in the measured intensity after the AMZI. All of these changes reduce the visibility, thereby reducing the secure key rate.

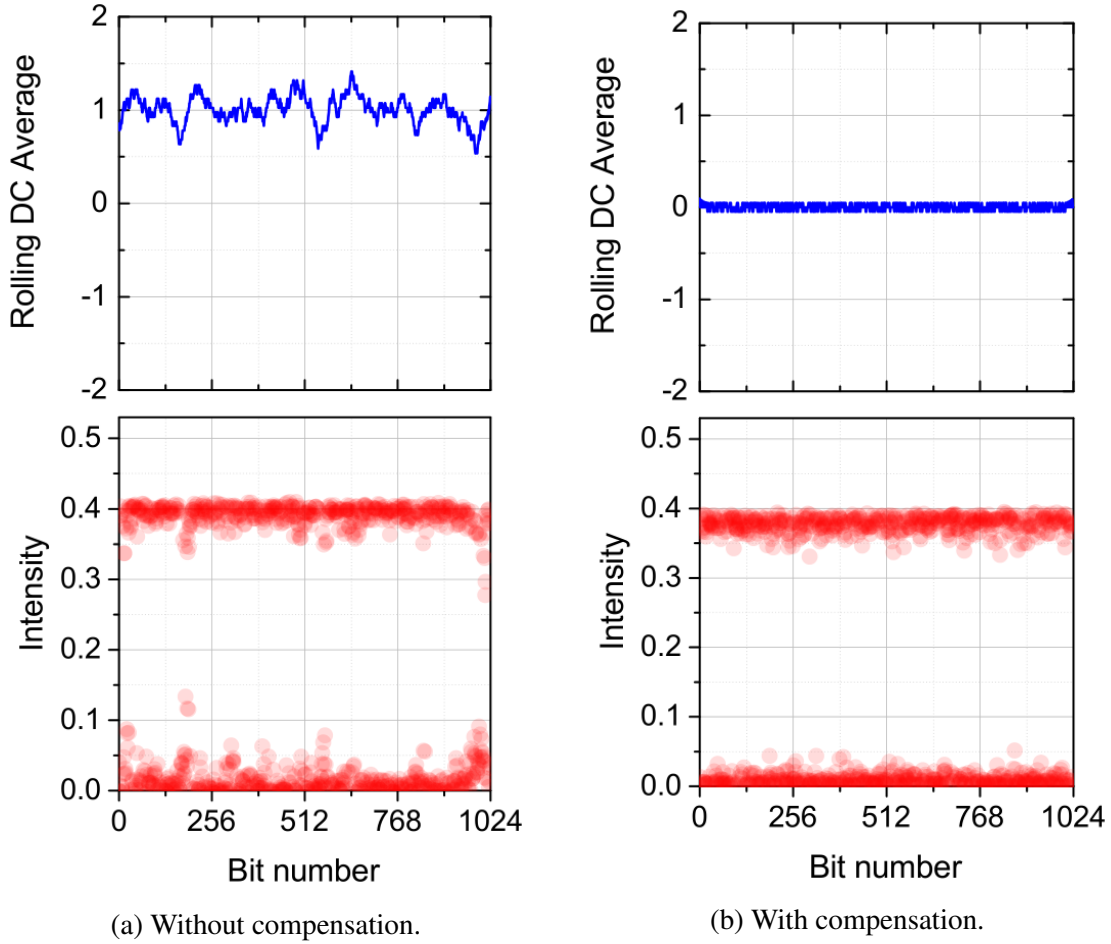
The input pattern should be altered to remove any DC shifts in the phase preparation laser, creating the scenario shown in Fig. 3.3b. It is possible to DC balance a pattern in classical communications across each clock period, for example using Manchester encoding. Here, each clock is separated into two bins, with one bin being in a high state and the other in a low state. The information is contained in whether the sequence is high-low or low-high. This



**Fig. 3.2 DPS oscilloscope traces.** *For cases where the signal is compensated and uncompensated. a) Electrical signal applied to the master laser. b) Optical signal from the master laser. c) Direct measurement of the optical system output. d) and e) Complementary outputs from both arms*

style is not possible using the directly-modulated transmitter, however the pattern can be DC balanced across a number of bit periods by alternating the  $\pi$  phase shift sign above and below 0, as demonstrated by the lower trace in Fig. 3.2. If a  $\pi$  phase shift has been encoded, the next time a  $\pi$  phase shift is required, a  $-\pi$  shift is instead given. This is exactly equivalent

to encoding a  $\pi$  phase shift, however has the effect that the mean DC value for a sequence of repeated '0' bits is identical to that of a sequence of repeated '1' bits. The compensation reduces the QBER observed on the oscilloscope from 3.84 % to 1.72 %.



**Fig. 3.3 DPS DC Compensation.** *The rolling average of pseudorandom  $2^{10}$ -bit patterns (top), with the measured intensity of every decoded pulse (bottom).*

In order to find the correct modulation amplitude, a random DPS pattern is input to the system and the pulse intensity is measured as the AMZI phase is varied, as shown in Fig. 3.4. This gives two sinusoidal curves, with a phase difference dictated by the modulation amplitude. The correct amplitude for the modulations is equal to the one that gives the best QBER because it is when the bits are maximally separated. This is the case in the aforementioned figure, which also shows the two curves crossing at an average intensity of one half.

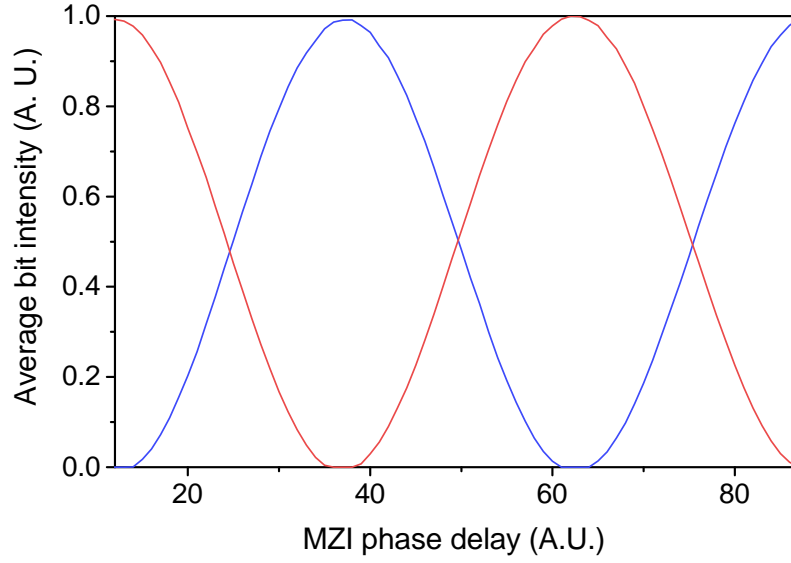


Fig. 3.4 **DPS bit intensity with AMZI phase.** The peak intensity of the pulses is recorded by an oscilloscope as the AMZI is tuned about  $3\pi$ .

### 3.3.3 Results and discussion

The experimental key rates derived using Eq. 3.1 and implemented using the directly-modulated quantum transmitter are shown in Fig. 3.5. The QBER and secure key rates follow the theoretical curves well, with a drop off around 50 dB as the QBER rises above 4 %. The base QBER used in the simulation is 1.70 %.

The DPS protocol has been implemented by many groups in different variations. One example is the experiment by Shibata *et al.* [148] that demonstrated a positive secure key rate over a 72 dB channel. Their implementation uses an intensity modulator to carve pulses from a CW laser at 1 GHz and a phase modulator to encode the bits. The aim of this work is to achieve a secure key rate over long distances, hence the detectors are optimised for ultra-low dark count rates (0.01 Hz), thus giving them a low efficiency (2.2 %), meaning the secure key rates are low (around 10 kbps at 20 dB channel loss). The transmitter is able to achieve a QBER of 1.02 %, meaning the system would potentially outperform the directly-modulated transmitter, at the expense of increased complexity. The protocol has also been demonstrated using an actively mode-locked fibre laser at 10 GHz as the pulse source, with a phase modulator used for encoding [149]. Although the clock rate is five times higher than the one used in this experiment, they are unable to produce a secure key due to the high QBER of 9.7 % caused by intersymbol interference.

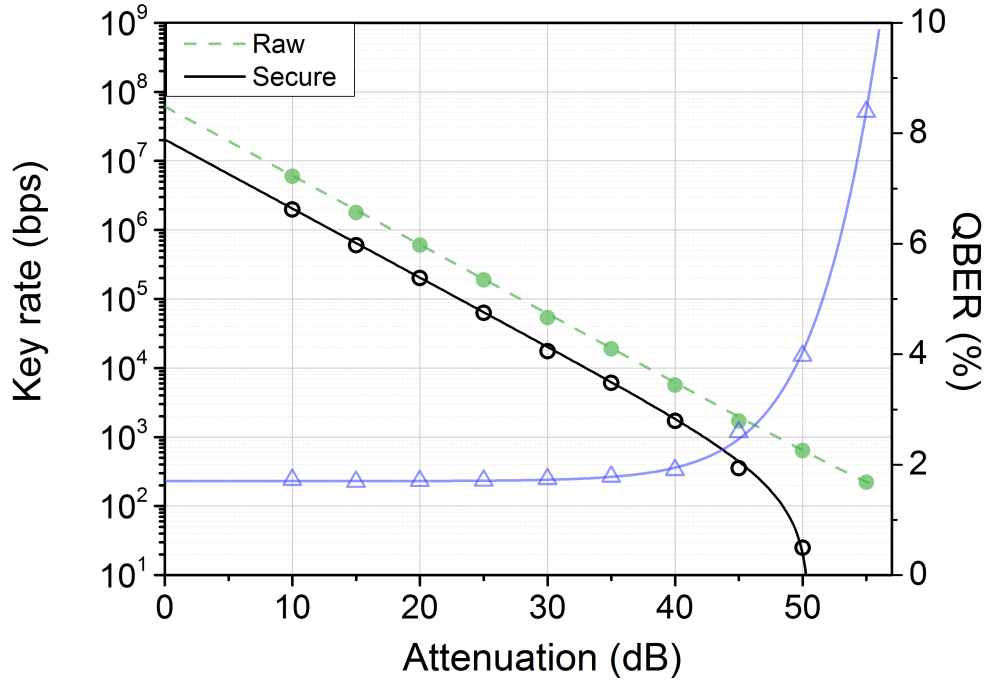


Fig. 3.5 **Experimental DPS results.** Key rates and QBERs extracted using a transmitted mean photon number of 0.18 photons per pulse.

### 3.4 Differential quadrature phase shift and BB84

Most experimental physicists would agree that it will remain impossible for Eve to perform coherent attacks in the foreseeable future, however one of the fundamental ideas behind QKD is that it should be future-proof. In that regard, it is wrong to ignore coherent attacks in security analyses. For this reason, theoreticians have worked on how to bolster the security of DPR protocols to the level of DV protocols such as BB84.

One potential method is known as round-robin DPS [150, 151]. Here, Bob uses an interferometer with multiple delays (the more he uses, the higher the secure key rate). He can choose which pulses to interfere, meaning Eve introduces errors when she guesses which pulses to interfere. Whilst a number of groups have come up with innovative implementations [152, 153, 154, 155], the receiver remains very impractical and the secure key rates are low.

Another method is known as the differential quadrature phase shift (DQPS) protocol. Here, the coherent signal is broken up into blocks with a globally random phase, allowing a modified BB84 protocol security analysis to be used. Two bases are used, X and Y, corresponding to the data basis and check basis. In the BB84 protocol, a signal and reference pulse are transmitted through the fibre with a globally random phase for the pair. This

block of two pulses has a mean photon number less than one, so the probability of multiple photons in the total block is very small. In the DQPS protocol, there are a number of signal and reference pulses in a coherent train, with a globally random phase for the entire block. Similarly to the BB84 protocol, the probability of any pulse pair having multiple photons is made very small when setting the mean photon number.

The BB84 protocol can be implemented using a phase-randomised pulse source and an AMZI, as shown in Fig. 3.6. This separates a single pulse into two time bins, modulating the phase between the two of them and allowing demodulation with an identical AMZI. The difficulty with this is that thermal fluctuations can create changes to the interferometer delay lengths. Feedback can be used to counteract this effect. To implement this feedback, stabilisation pulses are sent with the quantum signals, allowing the delay lengths to be continually measured and equalised. Another option would be to use a PLC AMZI (see Section 1.3.5), which are more stable. This is difficult in the transmitter, however, because high-speed PLC AMZIs are not commonly available and the commercially available devices use a heater to select the phase basis, limiting them to kHz speeds.

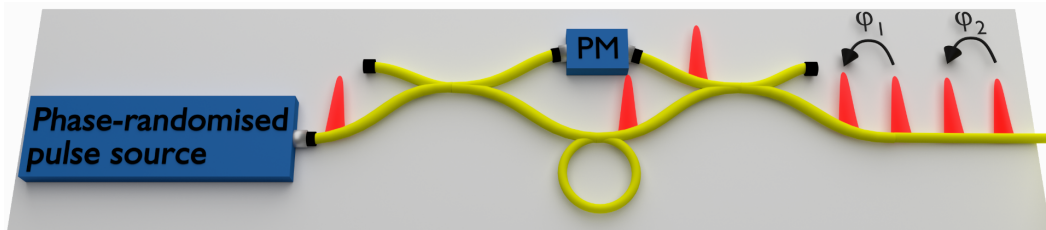


Fig. 3.6 **Potential BB84 transmitter.** A phase-randomised pulse source sends pulses into an AMZI with a phase modulator (PM) on one arm. This produces pulse pairs with a globally random phase and a differential phase between the pair ( $\phi_1$ ,  $\phi_2$ ).

The DQPS protocol, however, is more difficult to implement. An interferometer-based approach would require a multi-delay interferometer in the transmitter, a device that would be highly unstable and impractical. Another approach would be to use a standard DPS transmitter, then have an extra phase modulator to randomise the phase of blocks, as shown in Fig. 3.7. Whilst attractive in theory, this would require a high-speed source of perfectly random numbers and infinitely precise electrical modulation signals. For this reason, the DQPS protocol has not yet been experimentally demonstrated.

To allow a fair comparison between protocols, the same security analysis is applied to the BB84 and DQPS protocols in this chapter. Chapter 5 will look at the more efficient and secure decoy-state BB84 with a finite-key-size analysis.

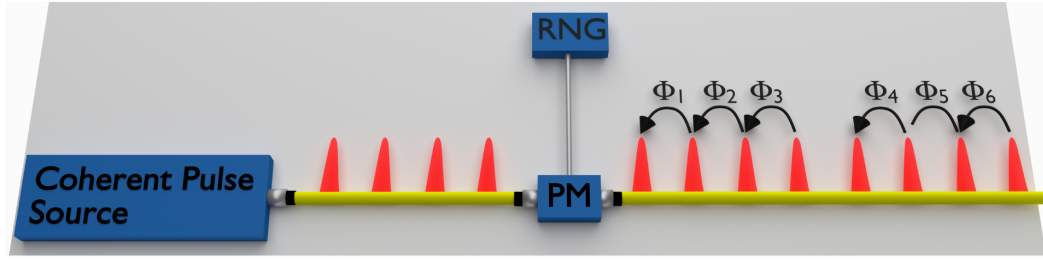


Fig. 3.7 **A Potential differential quadrature phase shift transmitter.** An extra random number generator (RNG) is fed into the phase modulator (PM) to provide the random phases for blocks in the differential quadrature phase shift protocol.

### 3.4.1 Theory

The steps to carrying out the DQPS protocol are outlined by Kawakami et al. and provided here for clarity [156]:

1. Alice chooses a random basis for each block of  $L$  pulses  $A_b \in \{0, 1\}$  with probabilities  $p_0$  and  $p_1$ .
2. Inside each block, she randomly chooses bit values  $A_l \in \{0, 1\}$ . The state can be described as the tensor product over all states in the block:

$$\bigotimes_{l=0}^{L-1} |e^{i\theta(A_b, A_l)} \sqrt{\mu}\rangle, \quad (3.2)$$

where

$$\theta(A_b, A_l) = A_l \pi + \frac{\pi}{2} A_b \quad (3.3)$$

3. Each block is given a random phase and sent to Bob.
4. Bob uses an AMZI with a one-bit time delay for phase measurement in a random basis for each block  $B_b \in \{0, \pi/2\}$ , again with probabilities  $p_0$  and  $p_1$ .
5. Bob records when he measured clicks and what their outcomes are. After detecting a click, he ignores any further clicks inside that block. If both detectors click at the same time, he randomly assigns a bit value.
6. Bob communicates his measurement times to Alice, allowing them to share a sifted key and then to perform error correction and privacy amplification.

The steps for BB84 are identical, but the block size is set to a constant  $L=2$ .



The security analysis uses a concept known as tagging, where all the qubits that Eve has full knowledge of are ‘tagged’. It is assumed that all multi-photon pulses are ‘tagged’ and are thus removed from the final key. This parameter can be measured in principle by Alice performing a projective measurement of the total photon number in a pair. The tagging technique must be modified slightly to work with the DQPS protocol, because a pulse-pair is defined only after Bob performs his measurement, whereas in BB84 it is always clear because only one pulse-pair exists. This parameter is now the probability of a single block having two or more photons distributed in a single pulse, or in two adjacent pulses. It is too late for Alice to make this photon measurement by the time Bob has performed his measurement, thus the security proof assumes Alice stores auxiliary qubits to perform a photon number measurement when she knows Bob’s measurement time. In reality, the tagged photon rate  $r_{tag}$  is statistically determined using the mean photon number  $\mu$  and the block length  $L$ :

$$r_{tag} = 1 - \sum_{m=0}^{\lceil L/2 \rceil} e^{-\mu L} \mu^m \frac{(L+1-m)!}{m!(L+1-2m)!}, \quad (3.4)$$

where the fraction term is simply the binomial coefficient  $\binom{L+1-m}{m}$ .

This allows us to write the secure key rate as [156]

$$R_L = \frac{p_0^2}{L} \left( (Q - r_{tag}) \left[ 1 - h \left( \frac{E_Y}{Q - r_{tag}} \right) \right] - Q h \left( \frac{E_X}{Q} \right) \right), \quad (3.5)$$

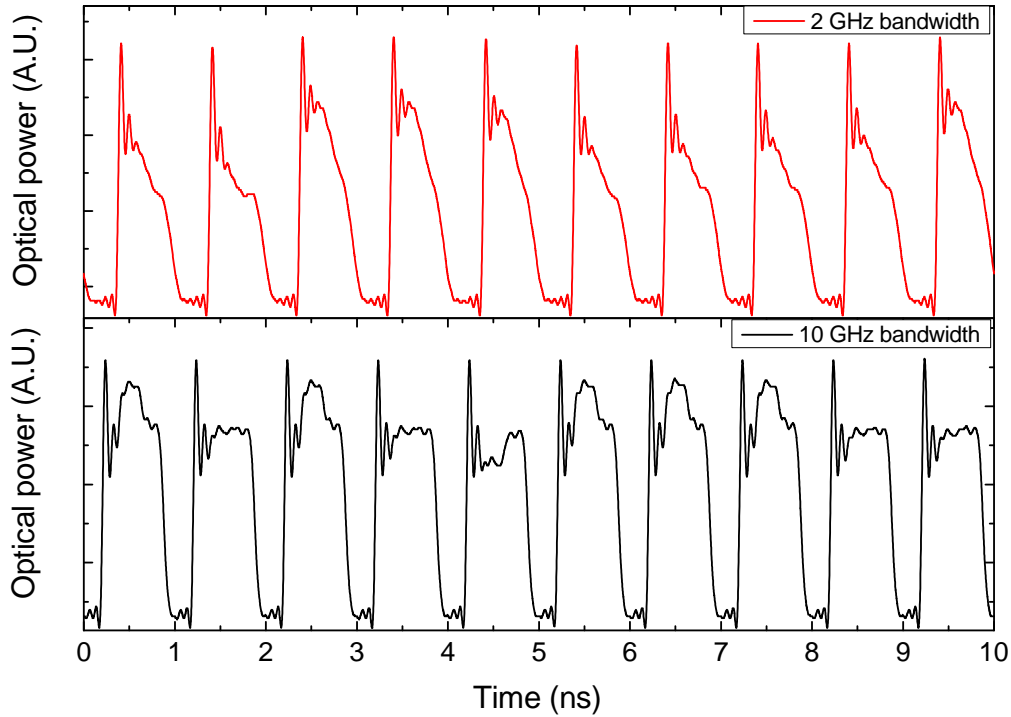
where  $p_0$  is the probability of Alice preparing a state in the data basis,  $Q$  is the total gain and  $E_{X,Y}$  are the errors in the data and check basis respectively.  $h(x)$  is the binary entropy function truncated to unity at input values over 0.5.

### 3.4.2 Implementation

A 2 GHz electrical square wave is applied to the pulse preparation laser for the DQPS and BB84 protocols, as with the DPS protocol, because no intensity encoding is necessary. The phase preparation laser signal must be modified from the DPS implementation, however, because phase randomisation is required. This can be implemented by driving the laser below threshold for a period of time, as described in Section 1.3.6. Below threshold, spontaneous emission is dominant, meaning that when the laser is driven above threshold, the starting phase is completely random and uncorrelated to any previous coherence.

A high bandwidth master laser is required to respond to the large swing of the phase-randomisation signal, whilst accurately providing the shallow phase modulations. A 2 GHz

master laser, for example, is unable to respond quickly enough to provide both, as shown in Fig. 3.8. This figure also shows that a 10 GHz master laser is able to faithfully produce the desired signals. The peak shown at the beginning of each pulse-pair period is due to the transient oscillations caused by the laser rapidly coming from below to above threshold. This produces oscillations that have a characteristic decay time. These transient oscillations can be seen to continue until the phase modulation pulse, meaning the first pulse of the pulse pair could have a different frequency and intensity to the second pulse. These oscillations could be minimised by using a higher bandwidth laser, although telecommunication wavelength lasers are not commercially available at much higher bandwidths than the one used. To combat this, the phase-randomisation down-time is reduced to 125 ps, ensuring these oscillations are not present when the first pulse is locked.



**Fig. 3.8 BB84 master laser optical outputs.** *Measured optical waveforms for a 2 GHz (top) and 10 GHz (bottom) master laser, with a pseudorandom BB84 pattern input. The down-time is 250 ps.*

A  $2^9$ -bit pseudorandom pattern is generated as Alice's key using Labview. This is used for all distances, even though the block length changes with distance, hence the block size is limited to  $L = 2^n + 1$ , where  $2 \leq n \leq 512$ . This is shown in Fig. 3.9. A Matlab simulation using Eq. 3.5, the base QBER due to phase encoding and detector efficiency enables the calculation of the optimal block size and mean photon number at each distance. A  $512/n$  bit

pseudorandom pattern is generated to decide the encoding basis for each block based on the probability of sending a ‘data’ and ‘check’ block.  $L$  is defined such that the first pulse will always be a reference pulse, so there are  $L-1$  useful time bins within the block. The phase preparation laser is then patterned to encode the pulses with the desired phase shifts.

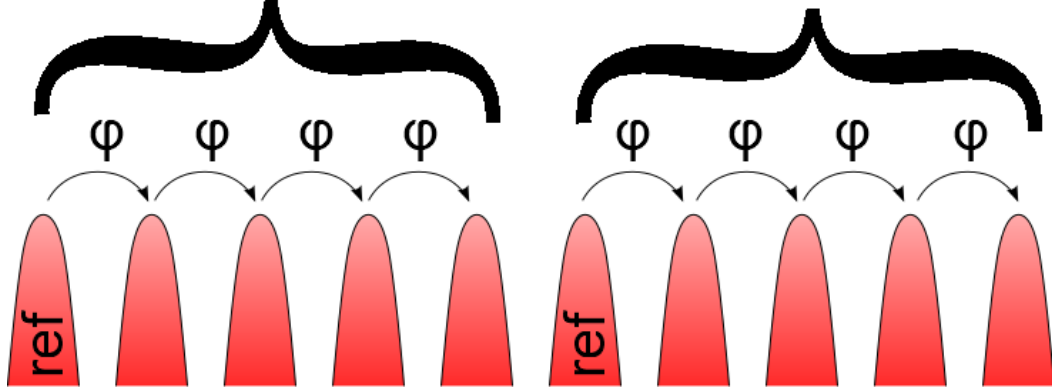


Fig. 3.9 **DQPS blocks.** Two example blocks for the DQPS protocol, with a block size  $L=5$ . This first pulse in all blocks is a reference pulse, hence only 8 useful bits are shown in the figure.

Once encoded, the output is sent through a polarisation controller to align it with the polariser in Bob’s AMZI. After this, the light passes through a spectral filter before attenuation with a variable optical attenuator to the desired mean photon number. For the majority of measurements, a second variable optical attenuator is used here to simulate the quantum channel attenuation. Data points at 20, 40 and 60 km are implemented with real optical fibre with a loss rate of 0.2 dB/km.

In this experiment, the AMZI loss is measured at 3 dB and the SNSPDs are measured with a total efficiency of 38.6 % and a dark count rate of 15 Hz. This analysis is purely about the transmitter, so no finite-key-size analysis is carried out, however to minimise the effect of any statistical fluctuations in the gain and QBER, measurements are carried out separately in each basis until  $4 \times 10^5$  counts are detected in each basis. At the largest channel attenuation, 22 dB, 600 s of acquisition time is required to obtain this block size.

The evolution of bit intensity with AMZI phase is given in Fig. 3.11. This shows the four encoded phases, each separated by  $\pi/2$ , as well as the random pulses. The random interferences have a constant value around 0.5 because the oscilloscope signal is averaged. The low QBER of the X and Y bases can also be inferred from this, as the extinction ratio of the states within each basis is high.

The probability of having a click in each time slot is simply the number of measured clicks divided by the laser repetition rate,  $P_{\text{click}} = n/n_{\text{rep}}$ . This allows us to define  $Q$  as the

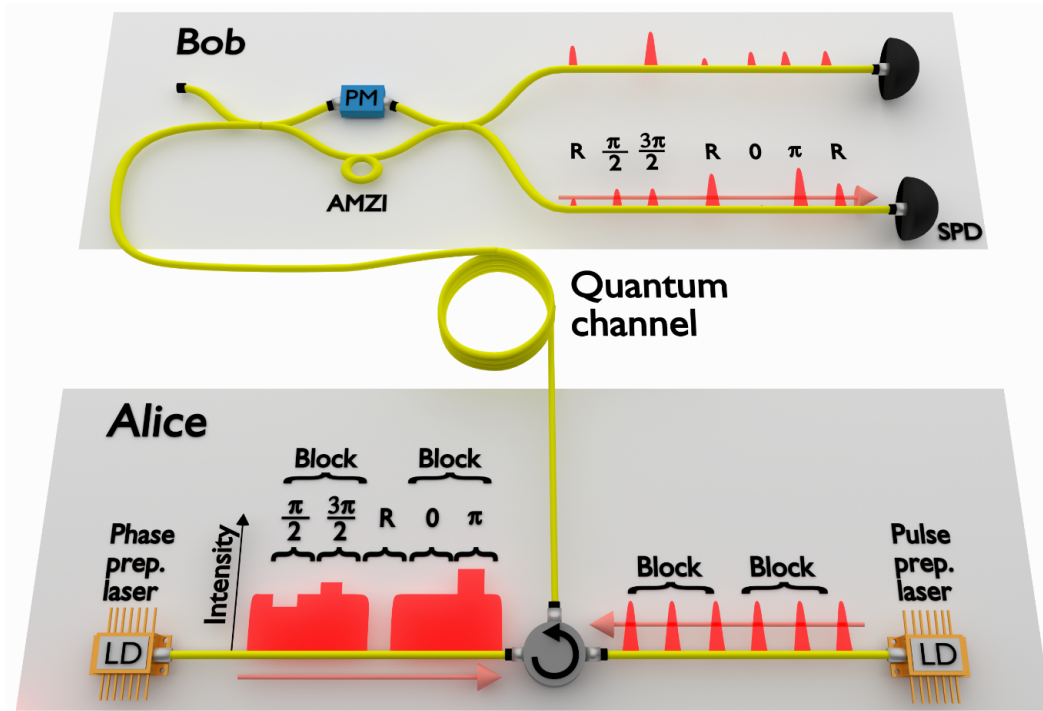


Fig. 3.10 **Differential quadrature phase shift schematic.** Blocks of size  $L=3$  are injected into the slave laser via a circulator in this figure. At practical system efficiencies, the optimal block length used is longer than this. Bob's measurement values are shown along their respective pulse intensities when measuring in the  $\pi$  basis.

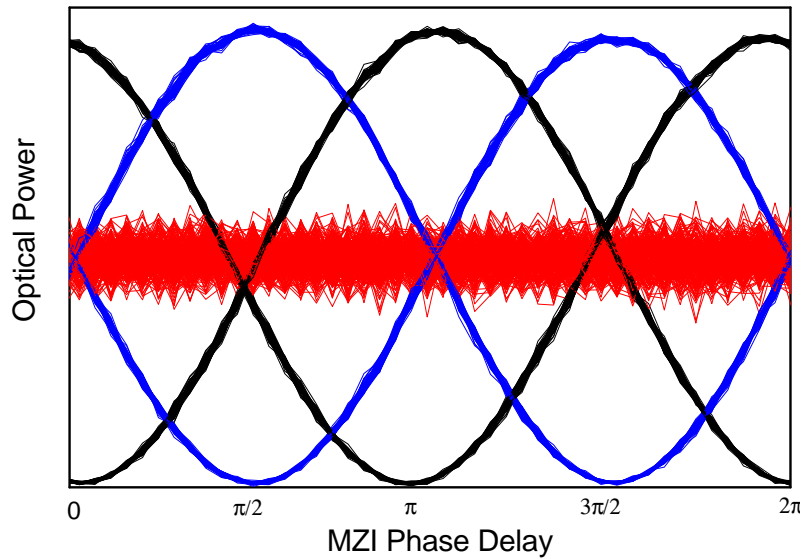


Fig. 3.11 **DQPS bit intensity with AMZI phase.** The peak intensity of the pulses is recorded by an oscilloscope as the AMZI is tuned about  $2\pi$ .

probability of having a single click in a block.

$$Q = 1 - (1 - P_{\text{click}})^{L-1}. \quad (3.6)$$

As described previously, if Bob measures a click for multiple pulses within the block, he only records the first one. This is used alongside the measured QBERs in the X and Y bases to calculate the secure key rate. The X (Y) QBER is measured indirectly through the visibility in the output histogram when the AMZI is set to measure in the X (Y) basis.

### 3.4.3 Results and discussion

The measured QBERs at different channel attenuations for the BB84 and DQPS protocols are shown in Fig. 3.12. This follows the expected trend, with an increase in QBER at larger attenuations due to the increased influence of dark counts. The base QBER for both protocols is low, at around 2.15 %. This base QBER is due to the visibility of the light source, as shown by Equation 1.3. This is slightly higher than the QBER observed in the DPS protocol due to the phase randomisation pulses disturbing the signal. The protocols would have the same QBER if more accurate electronics were used and the laser had a higher bandwidth.

The measured key rates are shown as a function of channel attenuation in Fig. 3.13. The raw counts shown are used alongside Eq. 3.5, Eq. 3.6 and the measured QBERs to calculate the secure key rate. Megabit per second secure key rates are achieved for both protocols at short distances. Using this transmitter, it would be possible to distil secure keys up to 22 dB in both protocols, which is equivalent to 110 km of standard optical fibre (with a loss rate of 0.2 dB/km).

Alongside the results for a variable optical attenuator as the quantum channel, three measurements are taken with real optical fibre, at distances of 20, 40 and 60 km. These all have a small amount of insertion loss, leading to their slight displacements from 4, 8 and 12 dB attenuation respectively. Group velocity dispersion, where different frequency components of light travel with different velocities, becomes an issue at longer distances. A pulse with a spectral width of 12 GHz would be broadened by 100 ps after 60 km of real optical fibre (based on a dispersion parameter of 18 ps/(nm km)). This would lead to an increased QBER, so dispersion compensated fibre is used. This introduces a negative dispersion along the fibre, reversing the broadening dispersion effects.

Another effect observed in real optical fibres is polarisation drift. Although phase encoding is used in this experiment, the detectors are polarisation dependent, and a polariser is placed after the AMZI. This means that polarisation feedback would be required in

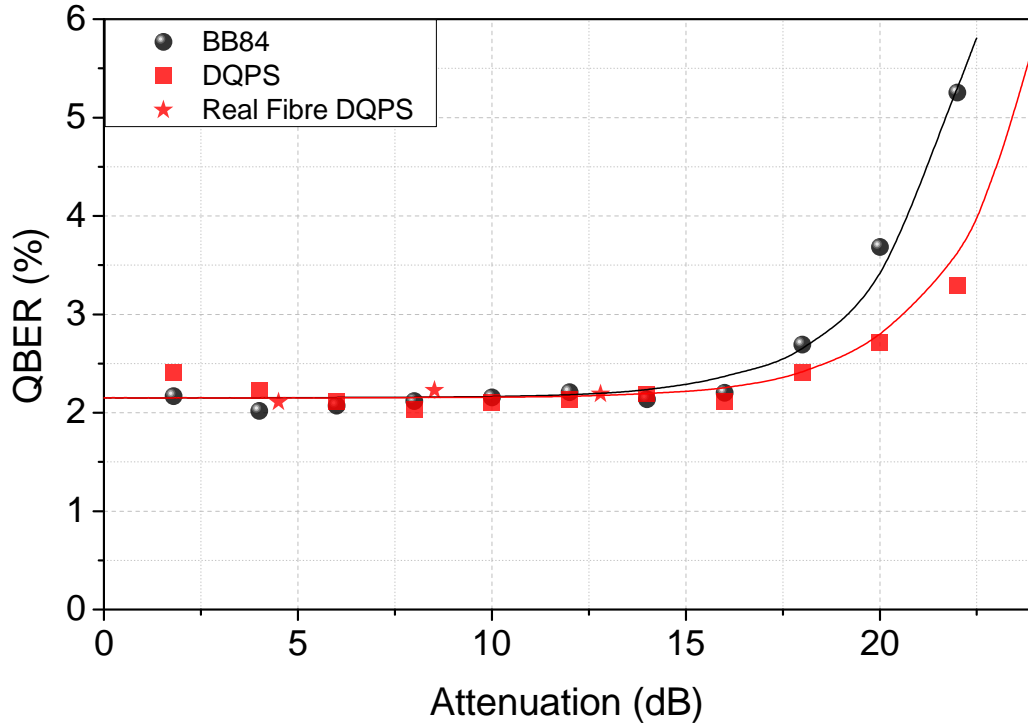


Fig. 3.12 **DQPS and BB84 error rates.** Measured *QBERs* at all experimental distances (symbols) shown alongside the simulated values (lines) based on the mean photon number used and the dark count rate.

deployed fibre to correct for any drifts along the fibre. In the current experiment, the fibre is in a laboratory so polarisation drift is not observed during the experiment.

The optimal DQPS block size increases with distance, starting at  $L=17$  for an attenuation of 1.8 dB, rising to  $L=129$  at an attenuation of 12 dB. These values are calculated at all attenuations using the key rate simulation with the measured system efficiency and base QBER. The secure key rate has an  $L^{-1}$  term, so intuitively it looks like a larger block size would be prohibitive. This term is counteracted by the terms  $Q$  and  $r_{tag}$ , which are both dependent on  $L$ . For a fixed mean photon number,  $Q$  will be higher for a larger block size because there are more potential time bins for a photon to be detected in. The tagging probability will also be higher for a larger block size for the same reason. This trade off between  $L$ ,  $Q$  and  $r_{tag}$  also explains why the DQPS secure key rate is higher than that of the BB84 protocol at all distances, with an average improvement of 2.71 times.

The optimal mean photon number,  $\mu$ , is also calculated for each distance using the key rate simulation. After being set, the actual values are measured, and are shown in Fig. 3.14.  $\mu$  decreases with attenuation due to Eve's improved ability to mask her measurements as

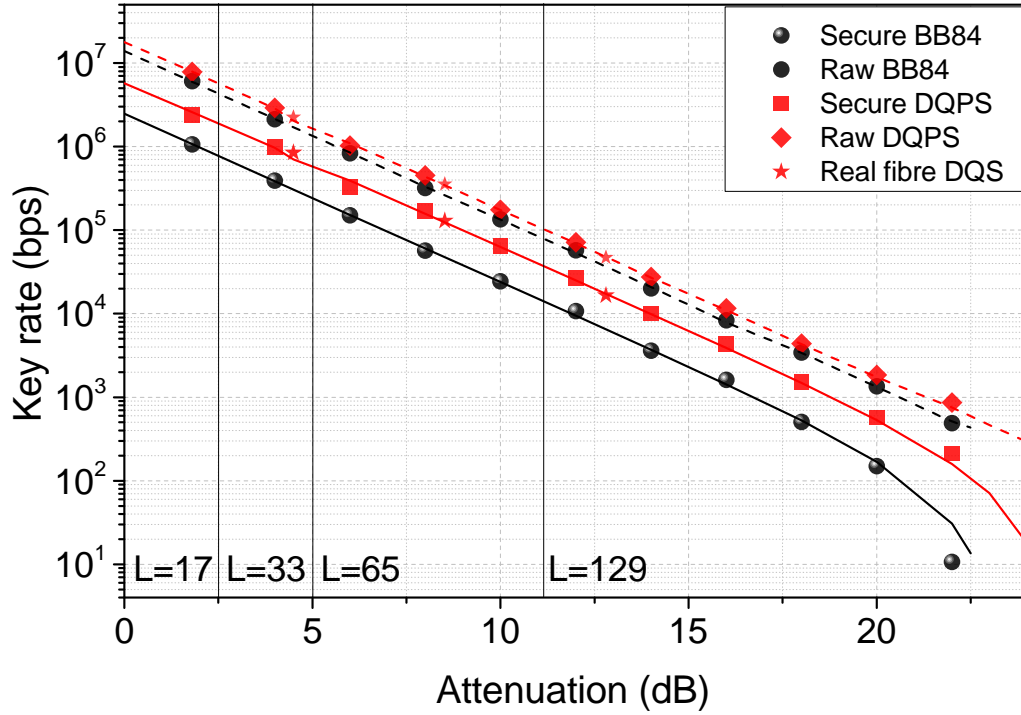


Fig. 3.13 **DQPS and BB84 key rates.** Secure key rates shown alongside the raw count rates for each protocol. Experimental data is given by symbols and simulated data based on the mean photon number are represented by lines. The DQPS block sizes,  $L$ , are also given.

noise by replacing the quantum channel with a completely lossless one. This would allow her to obtain more information from a photon number splitting attack.

The lack of an interferometer in Alice and the PLC AMZI used in Bob allow a demonstration of the excellent stability of the transmitter. To do this, the system is aligned once and then left to run. The lasers and AMZI are independently temperature controlled using a thermoelectric cooler with no active feedback. The single photon counts and QBER are then measured every 10 seconds with an integration time of 5 seconds over a period of three days. The results are given in Fig. 3.15. This shows an average QBER of 2.03 % and an average secure key rate of  $171.27 \pm 2.65$  kbps. There are no drops in secure key transfer over 72 hours, and the QBER does not rise above 3 % at any stage, even though the system is kept in a thermally unstable laboratory. The reductions in the raw key rate observed at various points are caused by errors in the single photon counting hardware. In a real-world system, this would allow 4.95 Gbits of secure key material to be shared between two users separated by 40 km of standard optical fibre. This demonstration reduces the system complexity by removing the need for time consuming stabilisation routines.

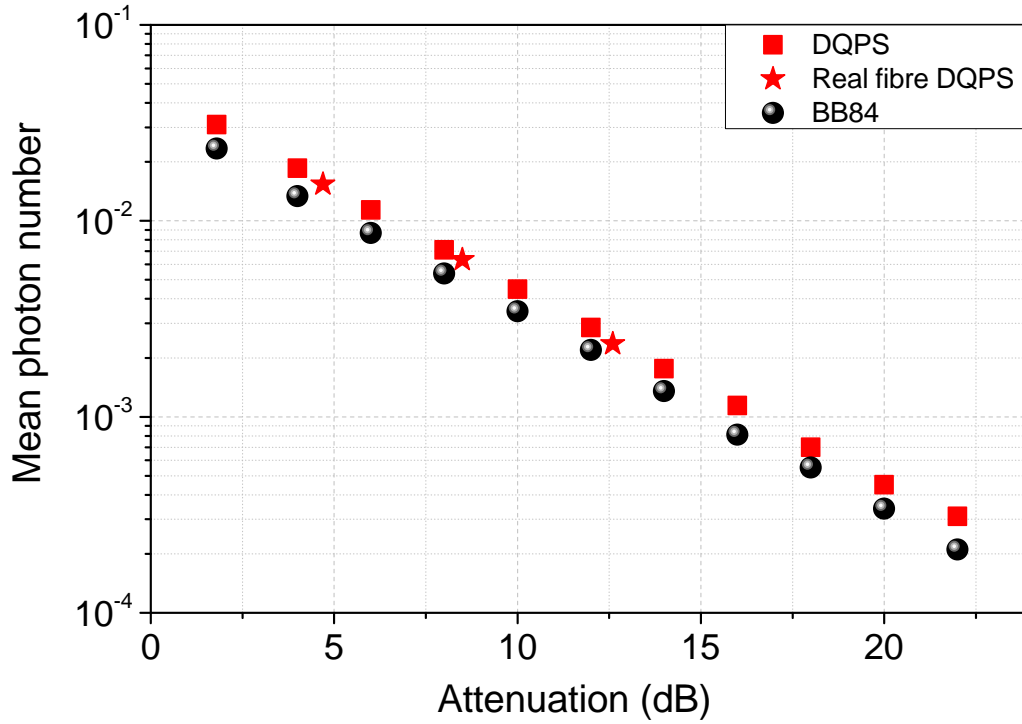


Fig. 3.14 **DQPS and BB84 mean photon numbers.** *The optimum mean photon number for each protocol at different channel attenuations.*

Whilst the QBER demonstrated in this BB84 implementation is comparable to that shown in other implementations, at around 2.5-5% [99, 101, 157], it is difficult to compare the secure key rates against other implementations. This is because an improved form of BB84, known as decoy-state BB84, allows for higher secure key rates over long distances, thus all experimental demonstrations since 2005 use decoy states. The decoy-state technique allows for a better estimation of the amount of single photons received by Bob, compared to the worst-case analysis given in this chapter. Developments in single photon detection technology since 2005 mean that the demonstration of BB84 in this chapter produces secure key rates orders of magnitude higher than those achieved a decade ago in other non-decoy-state demonstrations. The decoy-state technique and its implementation with the directly-modulated transmitter will be analysed in detail in Chapter 5, allowing for a comparison with more current implementations.



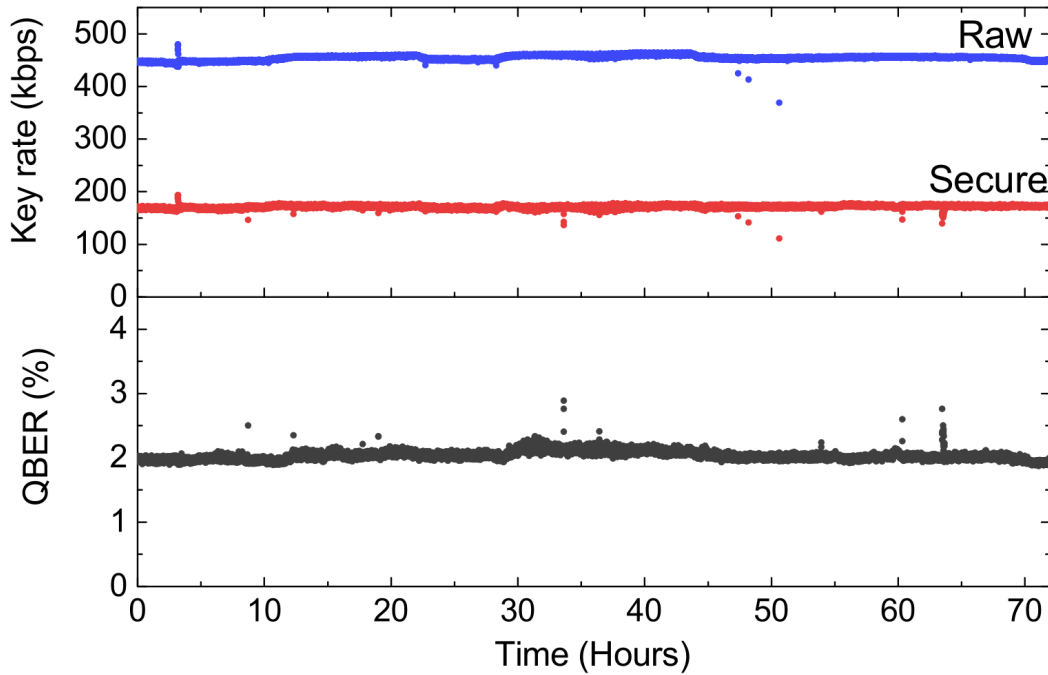


Fig. 3.15 **DQPS stability.** The key rates and *QBER* for a continuous *DQPS* measurement at 8 dB channel attenuation with no active feedback.

### 3.5 Summary

This chapter has shown the implementation of three phase-modulated QKD protocols with the directly-modulated quantum transmitter: the DPS, BB84 and DQPS protocols. The same transmitter hardware is used in all experiments, with changes to the driving signals enabling the different protocols. The *QBER*s demonstrated in the DPS and BB84 protocols are comparable to those found in many other implementations. This is the first experimental demonstration of the DQPS protocol. This protocol would ordinarily require a complicated transmitter, with either a multi-armed interferometer or the active phase-randomisation of every block. It was shown that the DQPS protocol is able to achieve a 2.71 times higher secure key rate to the BB84 protocol. This highlights the strong potential of the DQPS protocol, especially because implementing it with the directly-modulated quantum transmitter is just as simple as implementing the BB84 protocol.

The importance of compensating the electrical signal into the phase-preparation laser is shown. If this is not done correctly, the phase modulation is dependent on the mean DC level in each pattern region. For all protocols this can be done by alternating the sign of the  $\pi$  modulation pulse.

The stability of the transmitter is also demonstrated with 72 hours of continuous operation while implementing the DQPS protocol with a channel attenuation of 8 dB. The low QBER throughout the three days would allow a secure key just under 5 Gbits to be shared between two users.

# Chapter 4

## Intensity-modulated QKD

### 4.1 Introduction

This chapter looks at intensity modulation in classical communications and then outlines how it can be used for quantum communications in the form of time-bin encoding. The prominent QKD protocol that uses intensity encoding to share a secret key between two users, the coherent one way (COW) protocol, is then introduced and described. Finally, this protocol is implemented with the directly-modulated quantum transmitter described in previous chapters.

### 4.2 Intensity encoding

Intensity modulation is an obvious solution for encoding information using light. Even before fibre-optic communication, signal lamps and Morse code enabled long-distance communication between ships. Intensity modulation is not only easy to perform at the transmitter side, it is also simple at the receiver side because direct detection can be used.

In classical communications, amplitude-shift keying (ASK) is a common method of encoding data. This uses intensity modulation of a high-frequency sinusoidal wave (the carrier wave). Multiple bits of information can be encoded per pulse, with  $M$  intensity levels giving  $\log_2(M)$  bits of information. One form of ASK is on-off keying, where the carrier wave is either on or off for each bit-period. Pulse amplitude modulation is a similar method that uses a pulse-train instead of the carrier wave. These pulses are then independently modulated in the same manner as ASK and their amplitude encodes the information.

Practically, direct laser modulation is simpler and cheaper than using external modulators to encode data in the intensity of light. Unfortunately, it suffers a number of drawbacks in classical communication systems. The main drawback is that the modulation bandwidth is lower than that possible with external modulators. Along with this, the chirp caused by simultaneous wavelength modulation leads to complications with dispersion. These properties mean that high-speed intensity modulators are most regularly produced using an AMZI architecture. Here, input light is split into two paths and a phase-modulator (commonly Lithium Niobate) placed in one path changes the phase of the light, modulating the light intensity as the recombining waves interfere. In this manner, it is possible to precisely control the output intensity of light.

### 4.3 Time-bin encoding

BB84 uses qubits in orthonormal states within any conjugate bases. Eve has to guess a basis to measure the qubit because she does not know in advance which basis Bob has chosen to perform his measurement in. When she chooses the incorrect basis, the result will be non-deterministic due to the use of conjugate bases.

Whilst polarisation-encoded qubits could be used, they are prone to depolarisation and polarisation mode dispersion. This requires continuous high-frequency stabilisation to compensate for. Time-bin qubits are far more practical for fibre-based QKD applications. These take the form

$$|\psi\rangle = \alpha|0\rangle + e^{i\phi}\beta|1\rangle, \quad (4.1)$$

where  $\alpha^2 + \beta^2 = 1$ . There are two potential time bins, early and late, denoted by  $|0\rangle$  and  $|1\rangle$  respectively, with a phase difference between the two defined by  $\phi$ . This means the effective transmitted logical bit rate is half that of the clock rate. Three conjugate bases can therefore be used, as shown in Fig. 4.1. The X and Y bases have been described and used in Chapter 3. These are also known as the equatorial bases and are defined by  $\alpha = \beta = \frac{1}{\sqrt{2}}$ . The phase between the two pulses defines the qubit state, either 0 and  $\pi$  in the X basis; or  $\frac{\pi}{2}$  and  $\frac{3\pi}{2}$  in the Y basis. The global phase of each time-bin qubit must be completely random to ensure the security of BB84 and other similar DV QKD protocols.

Equally, the Z, or polar, basis can be used. Here,  $\alpha = 1$  and  $\beta = 0$  or  $\alpha = 0$  and  $\beta = 1$ , meaning the photon is either in the early or late time bin, with no phase encoding within the qubit. It is simple to show that the states within the basis are orthonormal and that a

measurement in the X or Y basis when encoding in the Z basis will give a non-deterministic outcome. Practically, the polar basis requires intensity modulation and no phase modulation.

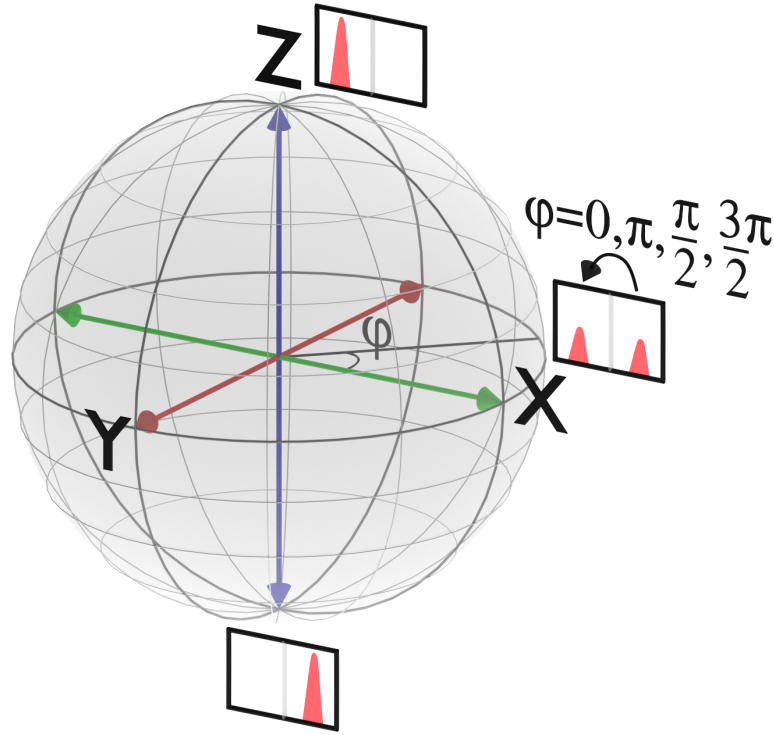


Fig. 4.1 **QKD states on the Bloch sphere.** The three potential QKD bases (X, Y and Z) are shown, with their states represented by arrows.  $\phi$  gives the phase encoding between the two pulses.

The Z-basis also has a number of benefits when used in QKD. Firstly, the QBER can be lower than with phase-encoding techniques due to high extinction-ratio intensity modulators and a receiver that is limited only by dark counts rather than interferometer visibility. This means that fewer bits are lost to error correction, increasing the secure key rate. Also, the receiver for the Z-basis is simple, using direct-detection, as in classical communications. SPDs are the most expensive part of a QKD system, and direct detection requires just a single SPD, compared to two with phase encoding. The main drawback is that the system complexity is increased if encoding in the X or Y bases is also required. This means that a phase modulator can be required as well as an intensity modulator. BB84 can in fact be carried out with two states in the Z basis, and just one in the phase basis [158].

The analysis above described the qubits as used for DV protocols such as BB84, however these bases can also be used for DPR protocols. Here, the pulse pair is not phase randomised, meaning the photon wavefunction is spread across a number of time bins. Security relies

on the maintained coherence in one of the phase bases and the qubit is defined as a tensor product across the time bins.

## 4.4 Coherent one way QKD

### 4.4.1 Theory

The COW protocol is a DPR protocol that exploits the Z basis, with the X basis being used occasionally to ensure the coherence has not been broken by an eavesdropper. The protocol is so-called because the phase between all photons is coherent, and the quantum signal travels only from Alice to Bob. Also, this protocol does not require equalisation of the Z and X basis mean photon number, which is required by three-state BB84 [158], simplifying the experimental implementation. The COW protocol has been used to distribute a secure key between two parties separated by 307 km of fibre, which was, until very recently, the longest distance for any two party protocol [86]. This is possible because the QBER can be made low in the Z basis, and also partially because the protocol has a weaker security than, for example, the decoy state BB84 protocol. As with the other main DPR protocol, differential phase shift QKD, the COW protocol has a simple implementation. This is shown in Fig. 4.2 and the steps are:

1. Alice randomly chooses which state to send from  $|\beta_0\rangle = |\alpha\rangle|0\rangle$ ,  $|\beta_1\rangle = |0\rangle|\alpha\rangle$  and  $|D\rangle = |\alpha\rangle|\alpha\rangle$ , where  $|\alpha\rangle$  represents a coherent state of light with mean photon number  $\mu = |\alpha|^2$  and  $|0\rangle$  is an empty, or ‘vacuum’ state.  $|\beta_0\rangle$  and  $|\beta_1\rangle$  are the logical bits, which she chooses with probabilities  $P_{\beta_0} = P_{\beta_1} = \frac{1-P_D}{2}$ , where  $|D\rangle$  is the decoy state.
2. Bob uses a 90:10 beamsplitter to passively route the majority of photons directly to an SPD, where he can measure the bit value. The remaining 10% of the photons are sent to an AMZI fixed in the X basis, allowing Bob to check the coherence. This ratio can be varied, however 90:10 gives a good trade-off between receiving a high number of photons for the key, whilst still receiving sufficient photons to measure the security.
3. Bob communicates his timing information to Alice and Alice tells Bob when she sent decoy states, allowing them to perform error estimation, error correction and privacy amplification.

Whilst the decoy states do reduce the secure key rate because fewer logical bits are transmitted, they are necessary because they allow the inter-bit interference to be measured.

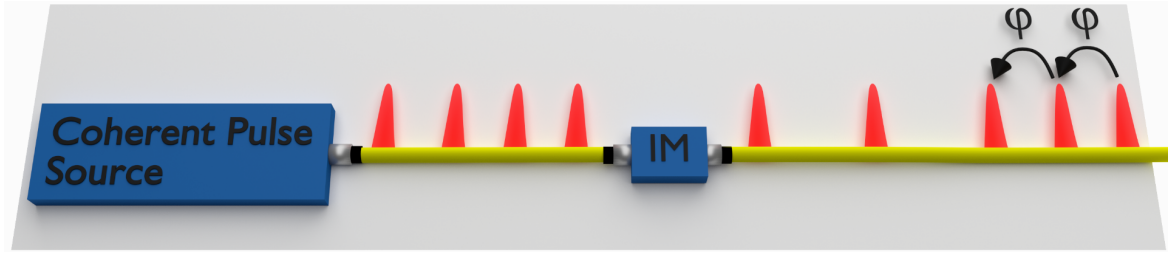


Fig. 4.2 **Potential COW implementation.** This uses a coherent pulse source (for example a carved CW laser) and an intensity modulator, IM, to encode the bit value.

Without the decoy states, the coherence can only be measured through the intra-bit sequence  $|\beta_1\rangle|\beta_0\rangle$ . This stops an attack by Eve where she coherently measures pulse pairs because she will have to choose between breaking the coherence in a logical bit or between two logical bits, decreasing the visibility if she chooses incorrectly. Eve doesn't know where the decoy pulses have been sent, thus she will inadvertently reduce the visibility. The decoy states also have the benefit of minimising the finite-key-size effect, because more pulses can be used to measure the visibility.

Korzh *et al* [86] outlines a finite-key-size analysis to derive the secure key rates against collective attacks with a total security parameter of  $\epsilon_{QKD}$ . This gives a secure key length of

$$L = n_Z \left[ 1 - Q - (1 - Q)h\left(\frac{1 - \zeta(V, \mu)}{2}\right) \right] - n_Z f_{EC}h(Q) - 7\sqrt{n_Z \log_2(\beta^{-1}) + \log_2(2\epsilon_{cor}\beta^2)}, \quad (4.2)$$

which can be divided by the time required to obtain the block to calculate the secure key rate. This equation can be broken into a number of parts. The first term is the key length after correcting for Eve's information, which is a function of measured block size in the Z basis ( $n_Z$ ), QBER ( $Q$ ) and visibility ( $V$ ). Here,

$$\zeta = (2V - 1) \times \exp(-\mu) - 2\sqrt{[1 - \exp(-2\mu)]V(1 - V)}. \quad (4.3)$$

$h(x)$  is the binary entropy function truncated to unity for  $x \geq 0.5$ . The second term is the reduction in key length after error correction using an algorithm with an efficiency  $f_{EC}$ . The final terms are the finite-key-size correction terms and  $\beta$  is chosen to maximise  $L$ , constrained by  $\beta \in (0, \epsilon_{qkd}/4)$ .  $\epsilon_{cor}$  is the probability that Alice and Bob do not share identical keys after the exchange.

Finite-key-size fluctuations are also taken into account in  $V$ , which deviates from the observed visibility by a term  $\Delta$  (i.e.  $V = V_{observed} - \Delta$ ):

$$\Delta = \sqrt{\frac{8(n_Z + n_X)\lambda(1-\lambda)}{n_Z n_X} \log \left( \frac{C\sqrt{n_Z + n_X}}{\sqrt{2\pi n_Z n_X \lambda(1-\lambda)\epsilon}} \right)}, \quad (4.4)$$

where

$$C = \exp \left( \frac{1}{8(n_Z + n_X)} + \frac{1}{12n_X} - \frac{1}{12n_X\lambda + 1} + \frac{1}{12n_X(1-\lambda) + 1} \right), \quad (4.5)$$

and  $\lambda = 0.5(1 - V_{observed})$ . This is a tail inequality, which essentially allows us to quantify a lower bound on the visibility.  $n_X$  is the measured block size in the X basis.

#### 4.4.2 Implementation

In order to perform the COW protocol with the directly-modulated light source, care must be taken to ensure the phase difference between the output pulses remains constant. If the phase preparation laser was removed from the system, it would still be possible to encode data in the Z basis by patterning the pulse preparation laser. This, however, would produce phase-randomised pulses, thus giving a random measurement result in the X basis. In order to provide a coherent phase, CW light from the phase preparation laser is injected into the pulse preparation laser. The visibility in the X basis is defined by the coherence of the phase preparation laser and the quality of the phase inheritance. The Z basis can then be encoded by patterning the pulse preparation laser.

The basic transmitter and receiver are shown in Fig. 4.3. A precise wavelength-tuneable CW fibre laser is used as the phase preparation laser for this demonstration, allowing the visibility to be maximised. A wavelength filter at the output port of the circulator removes any spurious noise, then an optical attenuator attenuates the signal to  $\mu = 0.1$  photons per pulse at Alice before being sent through the quantum channel to Bob. As with the DPS protocol, the receiver is passive and requires only two SPDs. This is possible because the AMZI can be tuned to measure in the X basis, such that SPD<sub>2</sub> is placed at the destructive output port. The visibility can then be calculated using the interfering peaks ( $N_I$ ) (i.e. a pulse-pulse sequence) and the fact that the non-interfering ( $N_{NI}$ ) (i.e. a pulse-vacuum or vacuum-pulse sequence) peaks will have four times fewer counts than an interfering peak.

$$V_{observed} = \frac{4N_{NI} - N_I}{4N_{NI} + N_I}. \quad (4.6)$$



The other detector directly measures the logical bits in the Z basis.

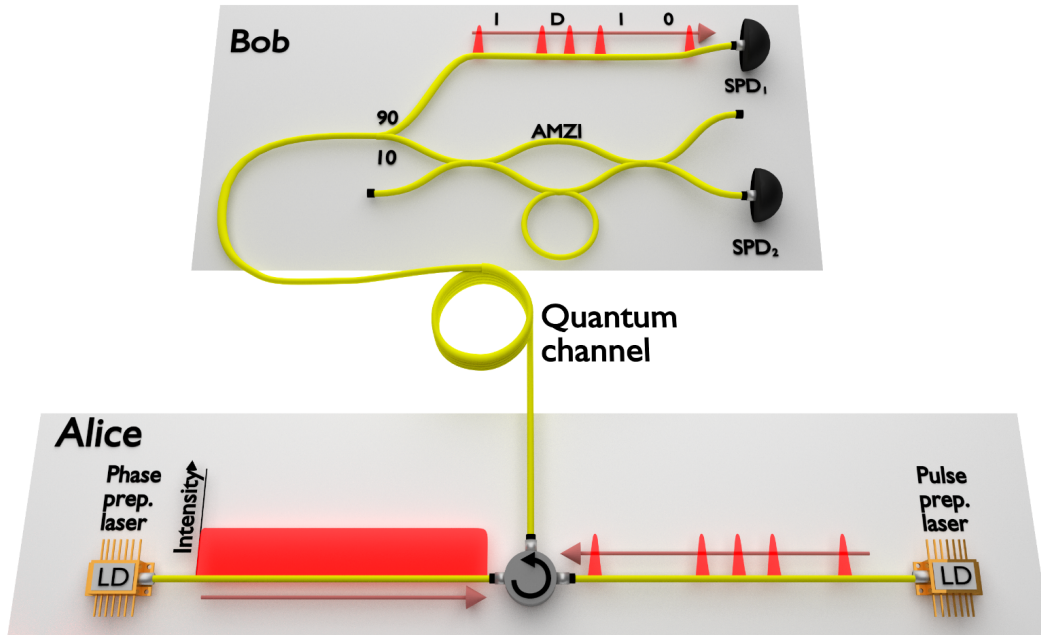


Fig. 4.3 **COW schematic.** A CW master laser is injected into a patterned gain-switched slave laser. Not shown are the filter and optical attenuator. This is then attenuated to the single photon level before being sent through the quantum channel to Bob. SPD<sub>1</sub> detects the time-bin encoded photons, and SPD<sub>2</sub> measures their visibility using a one bit asymmetric Mach-Zehnder interferometer (AMZI). The pattern shown in this figure is  $|\beta_0\rangle$ ,  $|\beta_1\rangle$ ,  $|D\rangle$ ,  $|\beta_1\rangle$ .

The evolution of the intensity of the different interferences in SPD<sub>2</sub> with MZI phase is shown in Fig. 4.4. This shows that the intensity of the non-interfering pulses remains constant, whereas the interfering pulse intensity varies as the measurement basis is rotated.

Patterning effects, where the intensity of a pulse is correlated with the intensity of the previous pulse, become a problem when working with intensity-modulated QKD systems. The COW security analysis is based on Eve obtaining a well-defined amount of information every time she makes a measurement on a qubit in the quantum channel. This amount of information changes if there is a patterning effect, because Eve could potentially gain information on the previous pulse. This requires either a change to the security analysis, which reduces the secure key rate, or preferably the removal of the patterning effect.

Patterning effects can be removed when working with an external intensity modulator by setting the DC bias to maximum transmission and then any modulation pulses are driven at the half-wave voltage. The transmission follows a sinusoidal relationship with applied voltage, so this modulation format works at the peak and trough of the transmission. Any

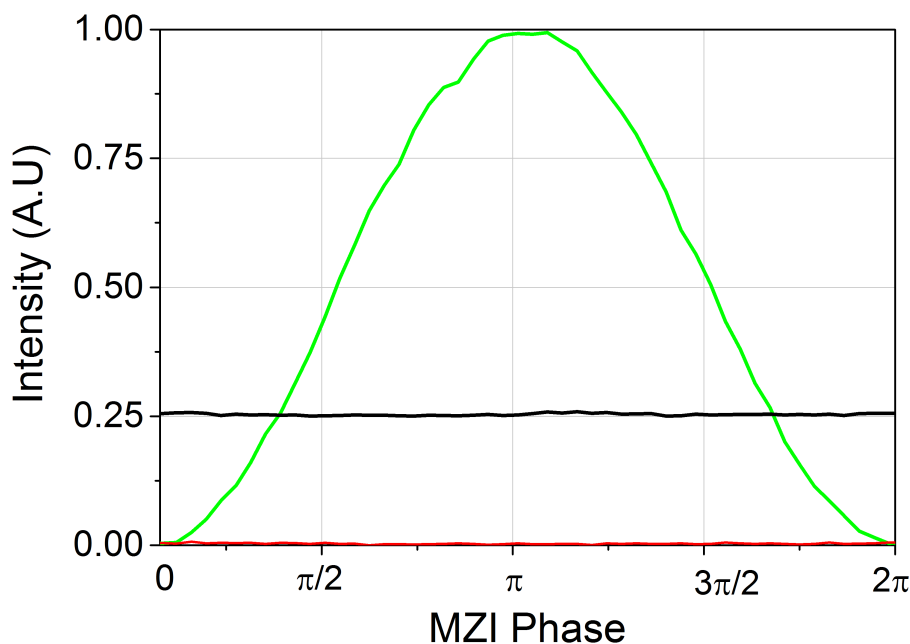


Fig. 4.4 **Bit intensity with AMZI phase.** *The intensity of every bit after the AMZI is measured on an oscilloscope as the measurement basis is rotated about  $2\pi$ .*

deviations in the applied electrical signal will thus have a minimal influence on the output voltage. This effect is further described in Section 5.4.2.

The issue must be tackled in a different manner for the directly-modulated transmitter. The finite electrical bandwidth of the system means that an electrical pulse after a vacuum pulse will have a lower voltage than an electrical pulse after another electrical pulse. In order to remove this problem, a finite electrical pulse is placed in every time bin. When a signal pulse is required, the electrical pulse is above threshold, whereas it is below threshold when a vacuum pulse is required. This ensures that each signal pulse is stimulated by the same electrical signal and there are no patterning effects. Before this compensation, the patterning effect can be as high as 5 %, however this is greatly reduced to 0.3 % with compensation, as shown in Table 4.1

Table 4.1 **Direct patterning effects.** *The signal ('s') pulse intensities extracted from a  $2^9$ -bit pseudorandom pattern input to the pulse preparation laser proceeding either another signal or a vacuum ('w') state. The average 's' pulse intensity is normalized to unity.*

Pattern	Average intensity of second pulse	Deviation from average (%)
s→s	$1.000 \pm 0.017$	0.00
w→s	$1.003 \pm 0.023$	0.30

A pseudorandom  $2^9$ -bit pattern is generated with a decoy pulse probability of 1 % and equal probability of logical bit values. The corresponding electrical pattern is then input to the slave laser, to produce 61.5 ps pulses at 2 GHz. A high extinction ratio of 29.4 dB is achieved between empty and non-empty pulses, leading to a low Z basis encoding error.

A variable attenuator acts to simulate the quantum channel loss, after which a beamsplitter directs 90% of the pulses to the Z basis and 10% to the X basis measurement. A heater in one arm of the AMZI is used to select the X basis and ensure that destructive interference occurs at the SPD. Superconducting nanowire SPDs are used, with a dark count rate of 10 Hz and an efficiency of 34 % at a wavelength of 1550 nm. A digitiser with 100 ps time bins logs the time of arrival of the pulses into 1024 separate bins to create Z and X measurement histograms for extraction of visibility, QBER and count rates.

### 4.4.3 Simulation

High count rates at short distances when using direct detection make it necessary to account for jitter when simulating the key rates. Although the signal time jitter is negligible due to the optical injection locking, jitter from the detectors is an issue. Detector jitter, the variation in determination of photon arrival time, is caused by the electronic circuitry and intrinsic effects inside the SNSPD active material. The electronic effect is caused by noise in the various components, such as amplifiers, which is well-characterised and can be minimised by manufacturers. It can also be caused by the electrical signal not being completely extinguished before a following pulse, leading to the following pulse being registered early. This would lead to a relationship between jitter and count rate. Very limited research has been done into the cause and conditions for these intrinsic effects [91], however it is also possible that they originate from the detector geometry [159]. After a photon impinges on the superconducting nanowire, the time taken for an electrical response to reach the electronics depends on the location of the event on the nanowire.

During SNSPD characterisation, a linear relationship between jitter,  $J$ , in seconds and count rate,  $C$ , in counts per second was observed, following

$$J = 3.595 \times 10^{-18}C + 5.871 \times 10^{-11}, \quad (4.7)$$

with an r-square value of 0.998. This means that the jitter is around 95 ps at count rates of 10 MHz, compared to 59 ps at count rates around 100 kHz. This increased jitter causes the measured QBER to increase at short distances, where the count rate is high, due to intersymbol interference. Pulses that belong in one time bin will be measured in the next

time bin. If the time bin is supposed to be a vacuum state, any extra photons will reduce the interference contrast, thus making the visibility and QBER worse. This extra jitter also means that more time bins must be collected at short distances in order to measure all the counts, further reducing the interference contrast.

The error rate simulations incorporate jitter by modelling its effect as a Gaussian distribution with standard deviation  $\sigma_J$ , added to a 61.5 ps Gaussian pulse,  $\sigma_P$ . These can be combined using

$$J_{tot} = \sqrt{\sigma_J^2 + \sigma_P^2}. \quad (4.8)$$

It is then assumed that each pulse is in the centre of its bin, allowing the proportion of the signal entering the next bin,  $I_{leak}$ , to be calculated using the cumulative density function of a normal distribution with standard deviation  $J_{tot}$ .

#### 4.4.4 Results and discussion

An example of the measurement results for the COW protocol is shown in Fig. 4.5. This shows both logical bits, alongside a single decoy pulse sequence. The top panel highlights the high interference contrast between signal and vacuum pulses that give such a low QBER in the Z basis. The bottom and middle panel show that consecutive pulse sequences will give interference, and also show that this interference contrast is not as high quality as in the Z basis. It can also be seen that the area under the constructively interfering pulses is four times higher than under non-interfering pulses. This is why the constructive interference shown in the bottom panel does not need to be measured in the experiment. It should be noted that the count-rate dependence on jitter is also present in this figure, with the pulses appearing more spread out in the top panel compared to the bottom two panels.

The measured QBER and visibility are shown along with the simulated values in Fig. 4.6. The experimental QBER follows the simulated trend due to jitter, where at short distances the count rate of around 10 MHz increases the jitter, and consequently the QBER. At short distances, it was necessary to consider a larger bin width experimentally, in order to detect all the expected counts. The simulation does not account for the difference in bin width, hence the fit is not perfect. The visibility is relatively unaffected by the increased jitter at short distances. This is because the count rate is lower in the X basis than the Z basis due to the 90:10 beamsplitting ratio and also the losses caused by the AMZI. Due to this, however, dark counts have a much larger impact on the visibility than on the QBER, with a drop-off observed at 25 dB.

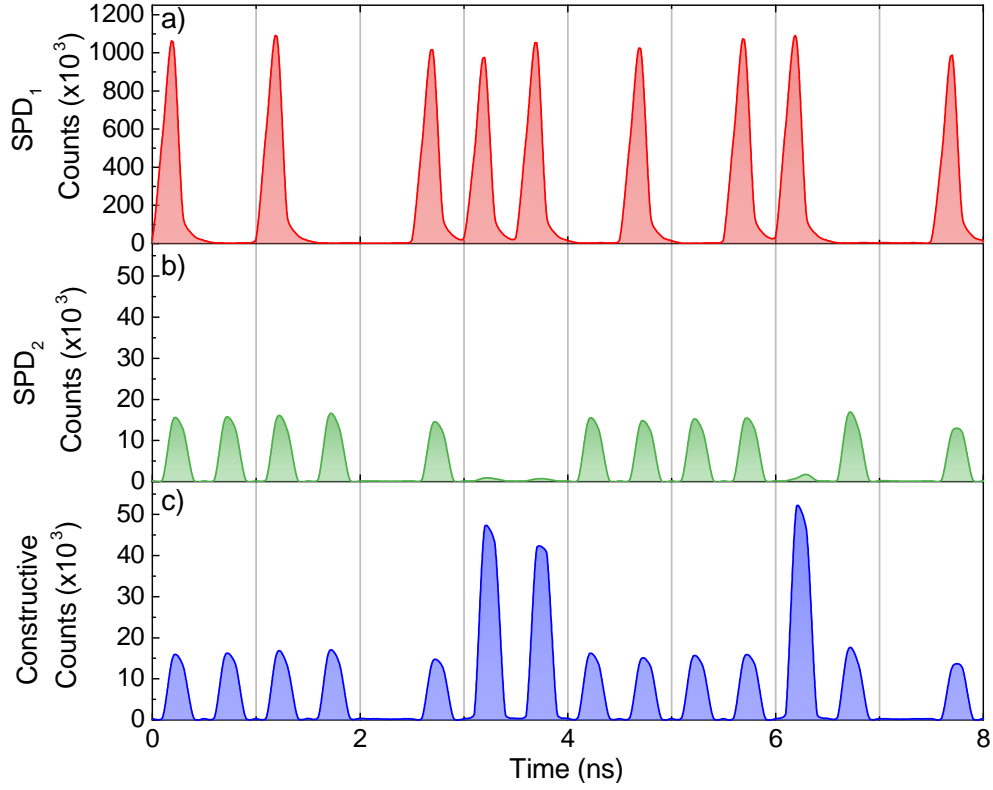


Fig. 4.5 **Measured COW SPD traces.** Signals received by bob in a) The Z basis; b) and c) the destructive and constructive arms of the X basis AMZI. The logical bit pattern shown, separated by vertical grey lines, is  $|\beta_0\rangle$ ,  $|\beta_0\rangle$ ,  $|\beta_1\rangle$ ,  $|\beta_2\rangle$ ,  $|\beta_1\rangle$ ,  $|\beta_1\rangle$ ,  $|\beta_0\rangle$ ,  $|\beta_1\rangle$ . The acquisition time is 60 s, the quantum channel loss is 15 dB and Alice is transmitting 0.1 photons per pulse.

The protocol is carried out until over  $2 \times 10^7$  counts are measured in the Z basis at each distance. This number of counts is chosen in order to minimise the finite-key-size effect, which is implemented with a security parameter of  $\epsilon_{QKD} = 10^{-10}$ . At longer distances, this requires an exponentially longer acquisition time, with 600 s necessary at 30 dB channel loss. Histograms, like those in the top and middle panels of Fig. 4.5, are collected, allowing for the extraction of count rates in both bases, QBERs and visibilities.

The secure and sifted key rates are shown in Fig. 4.7. The sifted key rate is simply the count rate in the Z basis with all decoy counts removed. The drop off in secure key rate at 35 dB is due to the decreasing visibility caused by the increasing influence of dark counts. This means that the finite-key-size effect is not the limiting factor, so increasing the acquisition time at long distances will not improve the maximum achievable distance. The key rate at 1.85 dB is lower than the theoretically expected value because a lower mean photon number is used in order to reduce the QBER by lowering the effects of time-jitter. The

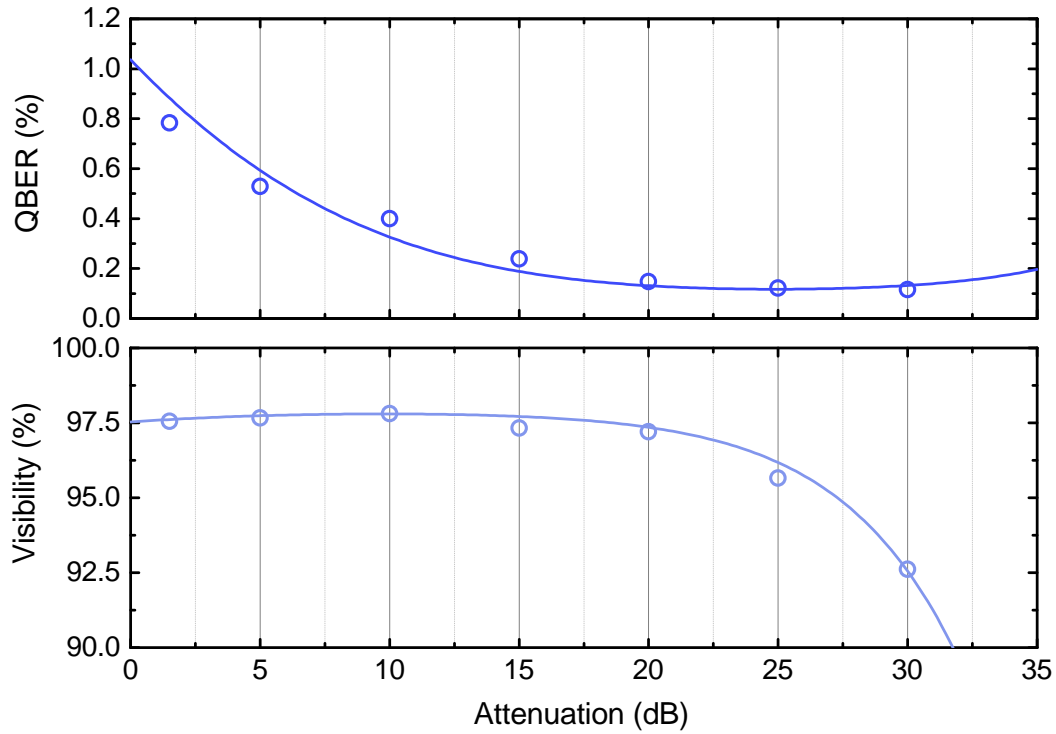


Fig. 4.6 **COW error rates.** *QBERs in the Z basis (top) and visibilities in the X basis (bottom). Experimental data is represented by symbols and theoretical data by lines. The theoretical analysis accounts for the increased detector jitter at short distances.*

mean photon number here is 0.07 photons per pulse, whereas it is 0.107 photons per pulse at all other distances. As well as this effect, the detection efficiency is also slightly reduced at higher count rates, explaining why the experimental points are under the theoretical line.

Whilst finite-key-size fluctuations are accounted for in this demonstration, they have only a small effect on the secure key rate. This is because the system has a high stability, thus can be carried out for a long time to minimise statistical variations in the measured counts and error rates.

Comparing Figures 4.2 and 4.3, the directly-modulated transmitter does not actually simplify the transmitter for the COW protocol, rather equalling the simplicity of other implementations. This being the case, it is still important that the transmitter can implement this protocol, because other implementations would not also be able to adapt to protocols that require phase-modulation and phase randomisation without changing the hardware. These results compare favourably to the state-of-the-art COW protocol implementation by Korzh *et al.* [86]. Their experiment uses a CW laser with an intensity modulator to carve out the desired pulses. This allows the researchers to achieve a higher visibility than that achieved in this thesis, of 98.4 %, compared to 97.5 %. Surprisingly, the QBER demonstrated in their

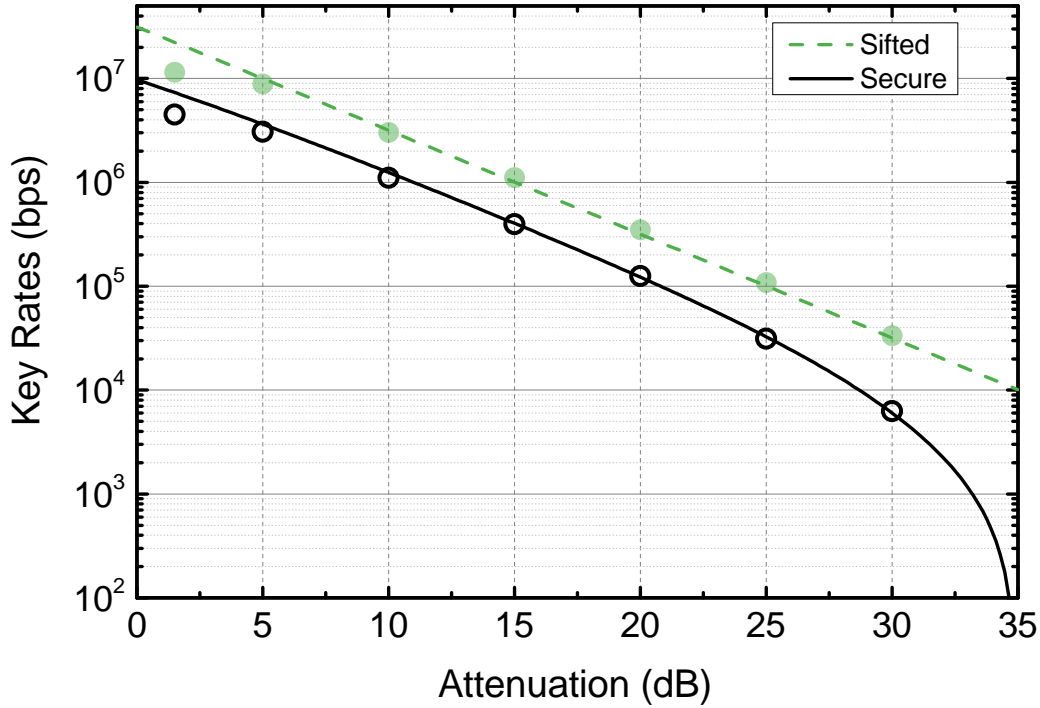


Fig. 4.7 **COW key rates.** Experimental (symbols) and simulated (lines) key rates. The secure key rate is calculated using a finite-key-size analysis with a block size of at least  $2 \times 10^7$  in the Z basis.

paper is worse than the QBER shown in this thesis, at 1.5 % compared to 0.2 %. The resultant key rates demonstrated in this thesis are higher than the paper, at  $1.08 \times 10^4$  bps compared to  $5.20 \times 10^3$  bps at 25.7 dB channel attenuation. This is due to the order of magnitude improvement in the QBER, as well as the higher efficiency detectors (34 % vs 20 %). Also, they are able to reach a channel attenuation of 51.9 dB with a positive secure key rate, whilst the demonstration in this thesis reaches only around 35 dB. This is due mainly due their usage of ultra-low dark count detectors (0.87 Hz) and long detector dead-time, but also due to their increased key collection time at long distances and the increased visibility.

The key rates are excellent when compared to the demonstrations of the DQPS and BB84 protocols in Section 3.4. This is especially notable when one notices the comparative simplicity of the passive receiver for the COW protocol, with just two SPDs. The main drawback is that the COW protocol has no security against coherent attacks. These require Eve to have an infinitely long quantum memory and a quantum computer to perform high-fidelity coherent quantum measurements. Whilst this may never be possible, it is important to be able to claim absolute security in a number of applications, which this protocol cannot provide.

## 4.5 Summary

This chapter has shown the first implementation of an intensity-modulated QKD protocol with a directly-modulated quantum transmitter. The transmitter hardware is identical to that used to implement the DPS, BB84 and DQPS protocols, with simple changes to the driving signals. Here, the phase preparation laser emits CW light to provide a coherent phase to the patterned slave laser pulses.

Accounting for finite-key-size effects, kilobit per second secure key rates have been obtained over a 30 dB quantum channel, limited by detector dark counts and acquisition time. At short distances, megabit per second key rates have been shown up to attenuations of 10 dB. These results are comparable to state-of-the-art demonstrations of the COW protocol.



# Chapter 5

## Concurrent phase and intensity modulated QKD

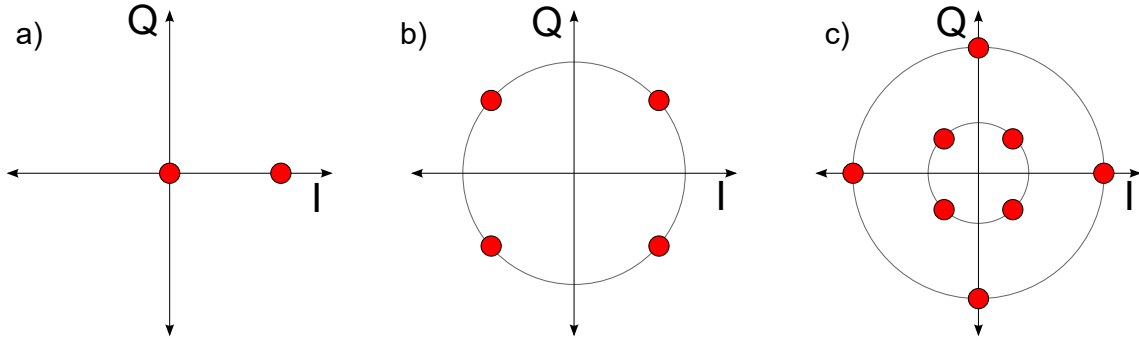
### 5.1 Introduction

The concept of separate phase and intensity modulation, alongside phase randomisation, has been explored in detail in the previous chapters. This chapter will work on bringing these concepts together to perform a single QKD protocol. It will also introduce the concept of decoy states and explore two different methods of real-time production of decoy states with the directly-modulated quantum transmitter.

### 5.2 Phase and intensity encoding

The idea of phase encoding was introduced in the form of phase-shift keying in Section 3.2, and intensity encoding in the form of amplitude shift keying in Section 4.2. These two techniques can be combined in a technique known as quadrature amplitude modulation (QAM) [160, pp. 160–166]. This uses concurrent amplitude modulation with phase shift keying to modulate more levels than is possible with the separate techniques, as shown in Fig. 5.1. Symbols in 256-QAM, for example, contain 8 bits of information, whereas PSK is limited to around 8 phase levels, containing 3 bits of information [161, 162]. The main drawback in moving to a higher number of levels is that the symbols become closer together on the constellation diagram, decreasing the signal-to-noise ratio [160, p. 164].

The two encoding methods can also be used together for QKD, as described in Section 4.3 [111, 158, 163]. In this case, the Z basis replaces either the X or Y phase basis. One



**Fig. 5.1 Constellation diagrams.** *Quadrature amplitude vs in phase amplitude for a) Amplitude shift keying, b) Quadrature phase shift keying and c) 8-quadrature amplitude modulation. Red circles indicate the modulation levels.*

such protocol implementing the Z basis is known as the polar BB84 protocol and is identical in theory to the phase-encoded BB84 protocol because the security is still based on the use of conjugate bases [59]. If Eve measures a qubit in the Z basis, she measures which time bin the photon is in, collapsing the photon wavefunction and destroying the phase information.

Practically, polar BB84 requires a more complex transmitter than phase-encoded BB84. The intensity of the X/Y basis must be reduced by one half to ensure it contains the same mean photon number as the Z basis. Also, a vacuum state must be modulated to encode the Z basis. These two requirements need an intensity modulator to faithfully produce three intensity levels, on top of the AMZI and phase modulator. The receiver, however can be simpler for polar BB84 because photons in the Z basis can be measured by direct detection. A completely passive receiver would require just three SPDs, compared to four in phase-encoded BB84. This is important because SPDs are usually the most expensive and complex component in QKD systems. An example receiver is shown in Fig. 5.2. A necessary requirement for the security of BB84 is that the detection probability is independent of the chosen basis [84, 164]. To satisfy this, an attenuator is added in the Z basis detection arm to balance out the loss of the AMZI.

On top of this, intensity modulation is vitally important to implement QKD with decoy states. Here, multiple photon numbers are transmitted by Alice. This chapter will focus strongly on how these decoy states can be implemented.

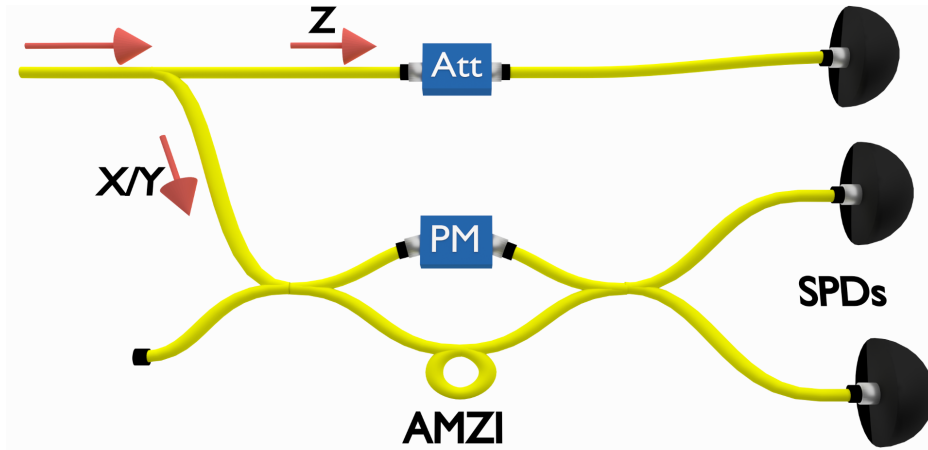


Fig. 5.2 **Intensity and phase receiver.** The polar (Z) basis is measured with direct detection and the equatorial (X/Y) bases are measured using an AMZI with a phase modulator (PM) on one arm. This phase modulator is only necessary in some implementations. An attenuator (Att) is placed on the polar basis detection arm.

## 5.3 Theory

### 5.3.1 Decoy states

As described in Section 1.3.3, the secure key rate of discrete variable protocols ordinarily scales very poorly with distance when weak coherent pulses are used instead of ideal single photons [57]. Fortunately, a method known as decoy-state QKD allows weak coherent pulse based QKD to have the same scaling as QKD with ideal single photons [87, 165, 166, 167, 168, 169]. In decoy-state QKD, pulses with a number of different mean photon numbers are prepared by Alice, rather than the previous case of a single mean photon number,  $\mu$ . This allows the two users to place a tight bound on how many detector events are caused by single photons and are thus can be used to generate a secure key. Previously they had to assume that every multi-photon pulse emitted by Alice causes a click in Bob's detectors, meaning they severely underestimate the number of single photon events. This method improves the scaling of the QKD secure key rate with transmittance,  $\eta$ , from  $O(\eta^2)$  to  $O(\eta)$ .

Whilst this improvement comes at the cost of requiring an additional intensity modulator inside Alice's transmitter, the price is often seen as small compared to the benefits. For this reason, the majority of current BB84 implementations use decoy pulses, including in quantum networks [170, 171, 172, 173, 174]. The advancement has allowed practical QKD systems to reach distances beyond 400 km and to achieve secure key rates over 13 megabits per second [99, 100].

Ideally, Alice would prepare signal states with a certain intensity, an infinite number of decoy state intensities (lower than the signal state intensity), and a vacuum state (a state with no photons) [166, 167]. Whilst this gives the highest asymptotic secure key rate, this situation is completely impractical. Not only would it be impossible to experimentally implement, it would also require a large amount of post-processing for reconciliation. A good trade-off is where Alice prepares three different photon intensities [80]. These are a signal state,  $s$ , a decoy state,  $v$ , and a vacuum state  $w$ , satisfying  $v \geq w \geq 0$  and  $s > v + w$ . This can be implemented using an intensity modulator in Alice.

The decoy-state technique gives Alice and Bob more information that can be used to estimate the single photon yield,  $Y_1$  used in their secure key rate calculation.  $Y_n$  is defined as the probability of Bob registering a detection event, given that Alice has prepared an  $n$ -photon state. The gain,  $Q_\mu$ , is the probability of Bob registering a detection event, given Alice is emitting weak coherent pulses with a mean photon number  $\mu$ :

$$Q_\mu = \sum_{n=0}^{\infty} Y_n \frac{\mu^n}{n!} e^{-\mu}. \quad (5.1)$$

Gain can be measured directly from experiments, because it is the number of received counts divided by the number of times an intensity state was prepared.

Decoy-state QKD with three decoy states gives three gain equations that can be used to bound  $Y_1$ . These can be solved numerically using linear programming, however analytical bounds are often used in practice. Similarly to how finite-key-size effects are approached, the worst case bounds are identified, which is the case with the lowest possible single photon yield,  $Y_1^L$ . Whilst the derivation has been shown in other works [80], it does provide some extra clarity on the improvements of using decoy states, hence a basic derivation is shown here.

First, a lower bound for the zero photon yield is identified,  $Y_0^L$ :

$$ve^w Q_w - we^v Q_v = v \sum_{n=0}^{\infty} \frac{Y_n}{n!} w^n - w \sum_{n=0}^{\infty} \frac{Y_n}{n!} v^n. \quad (5.2)$$

$$= (v - w)Y_0 + \left( v \frac{w^2}{2!} - w \frac{v^2}{2!} \right) Y_2 + \dots, \quad (5.3)$$

$$\leq (v - w)Y_0. \quad (5.4)$$

giving

$$Y_0 \geq Y_0^L = \frac{ve^w Q_w - we^v Q_v}{v - w}. \quad (5.5)$$

This allows  $Y_1^L$  to be found in a similar fashion:

$$Q_v e^v - Q_w e^w = \sum_{n=0}^{\infty} \left( Y_n \frac{v^n}{n!} - Y_n \frac{w^n}{n!} \right) \quad (5.6)$$

$$= (v - w)Y_1 + \sum_{n=2}^{\infty} \left( \frac{Y_n}{n!} (v^n - w^n) \right) \quad (5.7)$$

$$= (v - w)Y_1 + \sum_{n=2}^{\infty} \left( Y_n \frac{\mu^n}{n!} \times \frac{v^n - w^n}{\mu^n} \right) \quad (5.8)$$

$$\leq (v - w)Y_1 + \frac{v^2 - w^2}{\mu^2} \sum_{n=2}^{\infty} Y_n \frac{\mu^n}{n!} \quad (5.9)$$

Equation 5.9 can be simplified using Eq. 5.1:

$$\sum_{n=2}^{\infty} Y_n \frac{\mu^n}{n!} = Q_{\mu} e^{\mu} - Y_0 - \mu Y_1. \quad (5.10)$$

Substituting this back into Eq. 5.9 and using Eq. 5.5 gives

$$Y_1 \geq Y_1^L = \frac{s}{sv - sw - s^2 + w^2} \left( Q_v e^v - Q_w e^w - \frac{v^2 - w^2}{s^2} (Q_s e^s - Y_0^L) \right), \quad (5.11)$$

providing an equation with only experimentally measured quantities.

One assumption in decoy-state protocols is that the decoy and signal states are indistinguishable, meaning they must have identical spectral and temporal properties. Any deviation from this will give Eve some information about the intensity state, allowing her to perform an optimal attack that would require a modified security proof [175, 176].

### 5.3.2 Secure key rates

Experimentally, the received counts when Alice has prepared an intensity state  $\mu$  in basis A, given that Bob has measured in basis B,  $C_{\mu AB}$ , are measured and recorded. The QBER is calculated from the visibility in each basis and the error counts,  $EC_{\mu AB}$ , are calculated by multiplying the QBER by the number of counts. These quantities are scaled to account for the finite-key-size effects, giving a ‘worst case scenario’ secure key rate. This also allows us to quantify the security of our system using  $\epsilon_{sec}$ , defined as the probability the key is insecure. The upper and lower bounds are placed on  $C_{\mu AB}$  and  $EC_{\mu AB}$  using Hoeffding’s inequality for independent events [87]:

$$n^{\pm} = n \pm \sqrt{\frac{n}{2} \ln \frac{21}{\epsilon_{sec}}}. \quad (5.12)$$

The higher the security, the larger these fluctuations become, reducing the secure key rate compared to the asymptotic case. The bounds on the gain can then be calculated by dividing by the number of times Bob prepared each state.

For this implementation of decoy-state polar BB84 with finite-key-size effects, the security analysis outlined by Lim et al [87] is used. These equations are applied to the data gathered in the Z and X bases. The yields are bounded using a different method to that outlined in the previous section, however the main principle is the same. Here, the lower bound on the secure key rate that can be obtained is

$$R_L = [Y_{ZZ;0} + Y_{ZZ;1}(1 - I_E) - \lambda_{ErrC} - \Delta] / t, \quad (5.13)$$

where  $t$  is the time used to collect the block for processing,  $Y_{XX,ZZ;n}$  is the number of counts measured by Bob in the X or Z basis, given that Alice prepared an  $n$ -photon state in the X or Z basis respectively,  $I_E$  is Eve's information,  $\lambda_{ErrC}$  is the error correction leakage and  $\Delta$  is the finite-key-size correction term.

The zero and single photon yields in the Z basis are of particular interest because these are the photons that are used to distil the final key:

$$Y_{ZZ;0} \geq \frac{\tau_0}{v - w} \left( \frac{ve^w C_{wZZ}^L}{P_w} - \frac{we^v C_{vZZ}^U}{P_v} \right) \quad (5.14)$$

and

$$Y_{ZZ;1} \geq \frac{\tau_1 s}{s(v - w) - v^2 + w^2} \times \quad (5.15)$$

$$\left[ \frac{e^v C_{vZZ}^L}{P_v} - \frac{e^w C_{wZZ}^U}{P_w} - \frac{v^2 - w^2}{s^2} \left( \frac{e^s C_{sZZ}^U}{P_s} - \frac{Y_{ZZ;0}}{\tau_0} \right) \right]. \quad (5.16)$$

The single photon error rates are equally important:

$$e_{ZZ;1} \leq \frac{\tau_1}{v - w} \times \left( \frac{e^v EC_{vZZ}^U}{P_v} - \frac{e^w EC_{wZZ}^L}{P_w} \right). \quad (5.17)$$

$\tau_n$  in these equations is the probability of Alice preparing an  $n$ -photon state, which can be calculated using Poissonian statistics:

$$\tau_n = \sum_{\mu=s,v,w} \frac{\mu^n e^{-\mu} P_\mu}{n!}. \quad (5.18)$$

These n-photon quantities can also be calculated in the X basis by substituting the measured counts in Z for those in X.

$I_E$  in Eq. 5.13 is the maximum amount of information that Eve is able to obtain about the key, given the measured counts and error rates. It can be calculated for BB84 by applying the binary entropy function,  $h(x)$ , to the phase error rate in z,  $\phi_z$ :

$$1 - I_E = h(\phi_z) = -\phi_z \log_2 \phi_z - (1 - \phi_z) \log_2 1 - \phi_z, \quad (5.19)$$

where

$$\phi_z \leq \frac{e_{XX;1}}{Y_{XX;1}} + \gamma \left( \epsilon_{sec}, \frac{e_{XX;1}}{Y_{XX;1}}, Y_{ZZ;1}, Y_{XX;1} \right) \quad (5.20)$$

and

$$\gamma(a, b, c, d) = \sqrt{\frac{(c+d)(1-b)b}{cd \ln 2} \log_2 \left( \frac{c+d}{cd(1-b)b} \frac{21^2}{a^2} \right)}. \quad (5.21)$$

The leakage due to error correction,  $\lambda_{ErrC}$  is calculated in the Z basis using the total number of bits measured,  $C_Z$ , the efficiency of the error correction process,  $f_{ErrC}$ , set to 1.15 in this implementation, and the combined QBER of all intensity states,  $Q_Z$ :

$$\lambda_{ErrC} = C_Z f_{ErrC} h(Q_Z). \quad (5.22)$$

The final term in Eq. 5.13 is the finite-key-size correction term, equal to

$$\Delta = 6 \log_2 \frac{21}{\epsilon_{sec}} - \log_2 \frac{2}{\epsilon_{cor}}. \quad (5.23)$$

These epsilon terms define our certainty on the security and correctness of the key,  $\epsilon_{sec}$  and  $\epsilon_{cor}$ , respectively.

An extension of the BB84 protocol exists where the X, Y and Z states are used, known as the six-state protocol [12, 177]. This allows us to define Eve's information as

$$I_E = E_Z h \left[ \frac{1 + (E_X - E_Y)/E_Z}{2} \right] + (1 - E_Z) h \left[ \frac{1 - (E_X + E_Y + E_Z)/2}{1 - E_Z} \right], \quad (5.24)$$

where  $E_{X,Y,Z}$  is the QBER in the X, Y and Z basis respectively. This gives a slightly higher tolerance to the error than traditional BB84, allowing keys to be distilled over a longer channel attenuation.

Whilst six-state QKD has a better performance, phase-encoded BB84 is far more common than six-state QKD or polar BB84. This is because phase-encoded BB84 is the simplest to

experimentally implement. The AMZI implementation of phase-encoded BB84 is elegant because phase randomised pulses can simply be sent through the Mach-Zehnder interferometer to create the signal and reference pulse. Adding time-bin encoding into this situation would require an extra intensity modulator, further complicating the system.

## 5.4 Implementation

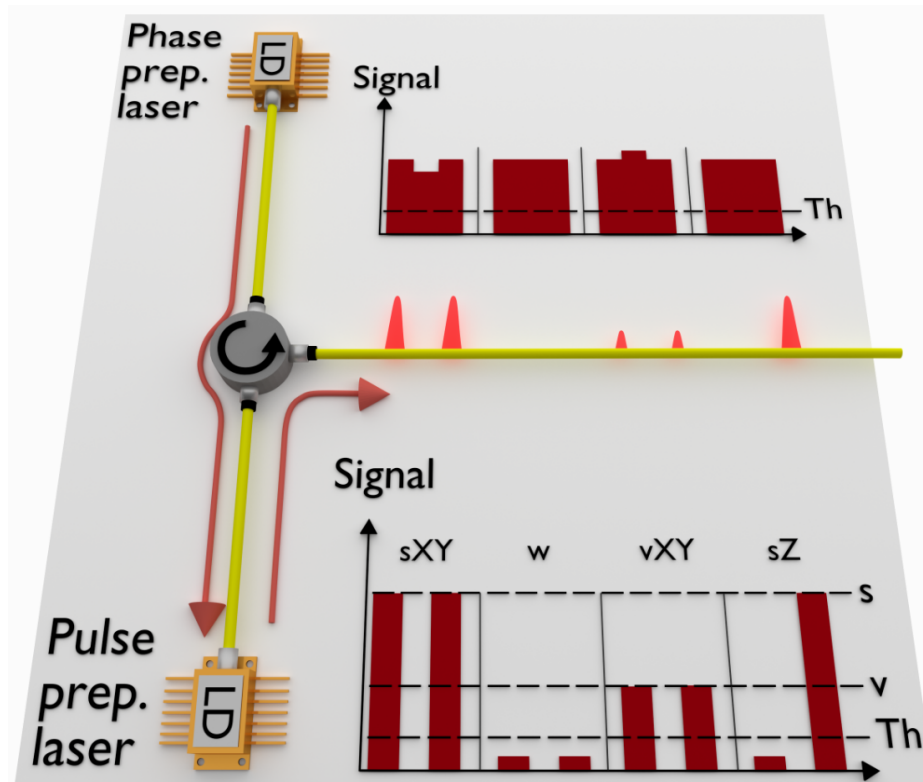
### 5.4.1 Directly-modulated decoy states

The first method of decoy-state production with the directly-modulated transmitter is to set three different driving current levels for the pulse preparation laser, depending on the desired pulse intensity. The signal pulse is produced by driving the slave laser far above its threshold and the decoy pulse by driving it above its threshold, but slightly lower than the signal pulse. The vacuum state can then be given by driving the laser below its threshold. This idea is shown in Fig. 5.3. As in Chapter 4, the presence of some electrical signal during the vacuum pulses is very important to reduce patterning effects. The voltage ratio between the applied electrical signals are 1 : 0.8 : 0.6 for signal:decoy:vacuum states.

This method of directly producing the decoy states is the most desirable option because it does not add extra components that would add to the complexity of the system. This allows the system to be more compact, lending itself more readily to on-chip devices, and also makes the transmitter less expensive. A final reason to remove the intensity modulator is that it removes any potential Trojan horse attack on this device. In this attack, Eve sends a bright pulse of light into Alice and measures the back reflections. The signal reflected from the active intensity modulator could contain information about the transmitted intensity state. One countermeasure is to simply have cascaded isolators at Alice's output so that Eve would have to shine in such a large amount of light that she would damage the optical fibre and turn her attack into a denial of service.

The main drawback in this method of producing decoy states is that their intensity is seen to depend on the previous pulse sequence. This is due to transient laser oscillations of one pulse overlapping with that of the subsequent pulse. The variation in decoy state intensities is also seen when using an intensity modulator, because the intensity modulator response to voltage is sinusoidal. The signal and vacuum states are produced by operating at the peak and trough, whereas the decoy state is between the two, giving a greater output uncertainty to imprecise voltages. Interesting theoretical research has been done into post-processing to remove any pulses that could leak information due to these patterning effects [178]. The





**Fig. 5.3 Directly-modulated decoy-state schematic.** *Six-state QKD with a lower driving level to directly produce decoy states.*

effect has been mitigated here by shaping the slave laser pulses with ‘shelves’, shown in Fig. 5.4. The result can be seen in Fig. 5.5. Whilst the results are not ideal, this method does indeed help to ensure that the pulses are all stimulated from a similar carrier and photon density level.

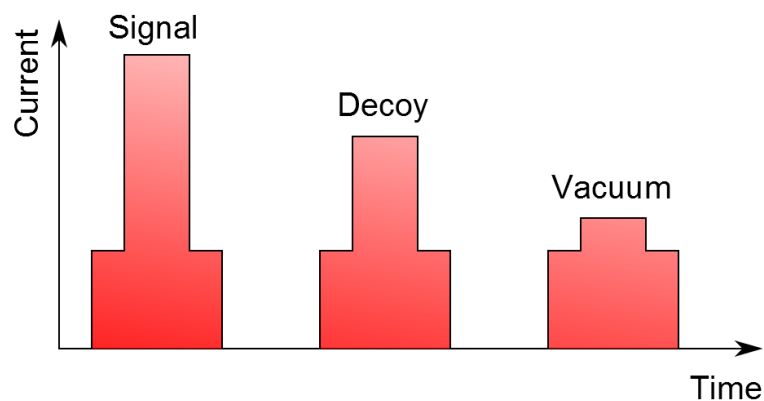
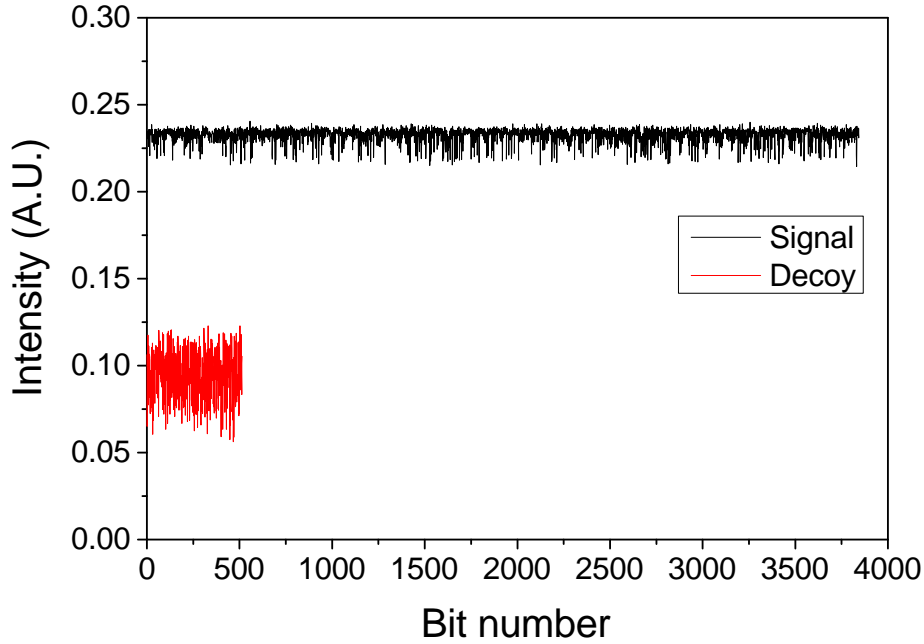


Fig. 5.4 **Slave signal ‘shelves’**. *The pulses are shaped to minimise the effect of transient oscillations from the previous pulse.*



**Fig. 5.5 Directly-modulated decoy-state fluctuations without compensation.** *Intensity fluctuations of all pulses in a 4096-bit six-state QKD pattern when the decoy states are produced using direct modulation. The signal state has a value of  $0.233 \pm 0.004$ , whereas the decoy state has a value of  $0.0955 \pm 0.014$ . There are fewer decoy measurements than signal measurements due to the increased probability of Alice sending a signal state.*

Another side channel to address with this implementation is that of a change in wavelength of the decoy states. The lower driving current means that the spectrum changes, meaning Eve could identify the intensity state using a wavelength measurement without introducing any errors. Whilst this is indeed true for the directly-modulated system, the effect can be mitigated by using a narrow linewidth (12 GHz) filter at Alice's output, as shown in Fig. 5.6. It is relatively easy to find similar spectral regions for such a narrow bandwidth, thus the output spectra overlap well. Loss due to the filter is not an issue because Alice has to further attenuate the signal to the single photon level.

A more pressing side channel is the timing of the signal and decoy states. The laser turn-on time is dependent on the amplitude of the applied current. A larger current will create population inversion more quickly, leading to a shorter turn-on time. What this ultimately means is that the directly-produced decoy states will occur at a slightly later time than the signal states, an effect that can be observed in Fig. 5.7. Interestingly, this figure also shows that the temporal profiles of the pulses are identical, thus there is no side channel if they can be made to overlap.

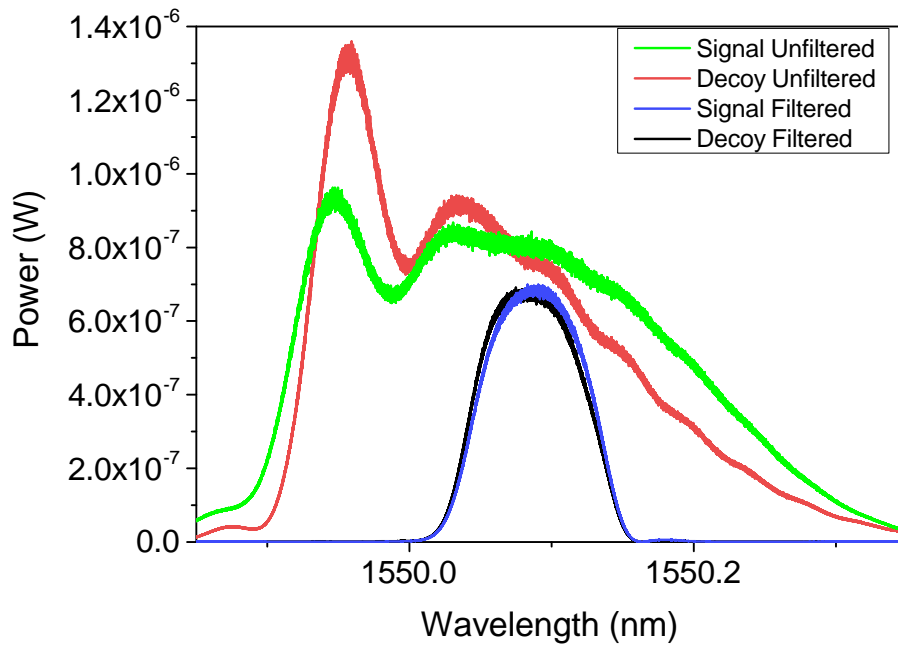


Fig. 5.6 **Directly-modulated decoy states spectra.** *Experimental results using a fixed 12 GHz spectral filter at 1550.08 nm. Both filtered and unfiltered spectra are normalised to have the same area.*

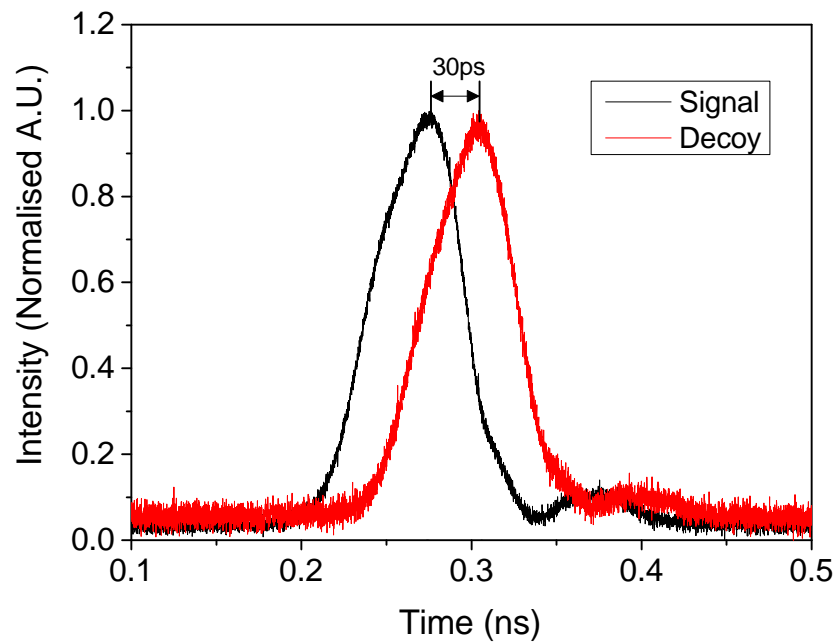


Fig. 5.7 **Directly-modulated decoy states time offset.** *Traces of the signal pulse and the decoy pulse. The decoy pulse is offset by 500 ps.*

The obvious solution to mitigate this effect is to simply shift the electrical decoy signals so the optical pulses occur at the same time as one another. The AWG being used has a sample rate of 24 GSamples/s, meaning the electrical pulses can only be shifted by multiples of 42 ps. In order to apply arbitrary time shifts, one AWG channel is used for the signal states and another is used for the decoy states. With careful delay alignment, these signals can be combined using a high-speed electrical combiner and input to the laser.

This solution worked well to produce a temporal overlap between signal and decoy states. Unfortunately, however, this led to a large increase in the aforementioned patterning effect, shown in Fig. 5.8. This is because the transient oscillations from the previous laser pulse become more influential as the pulse is moved closer to the previous pulse. Using the previous solution of adding ‘shelves’ to the pulses was not as effective here, leaving an unacceptably high variation in decoy state intensities.

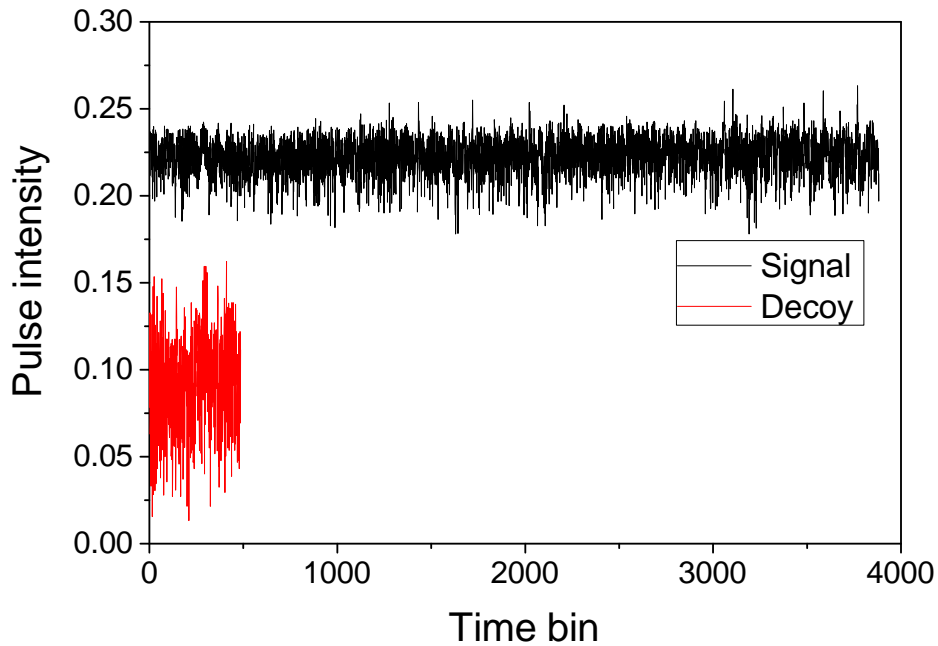


Fig. 5.8 **Directly-modulated decoy state fluctuations with compensation.** *Intensity fluctuations when the decoy pulse overlaps perfectly with the signal pulse. The signal state has a value of  $0.223 \pm 0.012$ , whereas the decoy state has a value of  $0.09428 \pm 0.029$*

#### 5.4.2 Externally-modulated decoy states

The most common intensity modulators for QKD systems are LiNbO<sub>3</sub>-based Mach-Zehnder interferometers with a phase delay induced in one arm by electrical modulation, as shown in

Fig. 5.9. These are known as Mach-Zehnder modulators (MZMs) and are used to produce the signal ('s'), decoy ('v') and vacuum ('w') states in decoy-state QKD. Here, the input light field is equally split into two different paths, one of which undergoes a phase shift before they are recombined. The value of the phase difference defines the intensity of the output, meaning the transmission can be controlled by applying electrical modulations to the phase modulation arm. The light travels in separate paths, thus each can undergo different phase shifts due to ambient conditions. This creates a drift in the output intensity that has to be removed using feedback to vary the DC voltage. MZMs can work up to very high bit rates by using a travelling-wave phase modulator, where a short electrical pulse travels through the device at the same speed as the light pulse [62]. Due to the birefringent nature of the  $\text{LiNbO}_3$  phase modulator crystals, input light must be linearly polarised along one crystal axis.

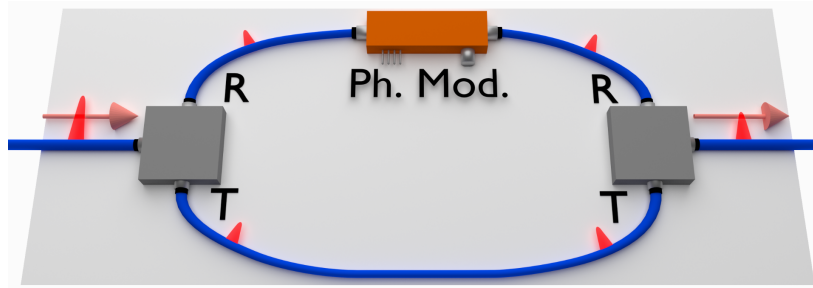


Fig. 5.9 **Mach-Zehnder modulator.** *Schematic of a Mach Zehnder modulator with a coupling ratio  $R:T$  and a travelling wave phase modulator.*

The patterning effect in these intensity modulators comes from their DC dependence and the sinusoidal response to voltage, as shown in Fig. 5.10 (black line). Small voltage fluctuations, shown as  $\Delta V$  in the figure, cause an insignificant variation in the output power,  $\Delta P$ , for 's' and 'w' states. The 'v' state is produced away from these points, however, where small voltage fluctuations can create significant changes in the output power. At high clock rates, the electrical signal does not have enough recovery time to reach the same base level before the next pulse, effectively changing the DC level. Also, the mean DC value of the input electrical pattern will vary slightly depending on the random pattern in that section, unless sophisticated encoding schemes are used. These effects both create voltage fluctuations in a random modulation pattern.

Current commercial intensity modulators are designed to achieve the maximum possible optical extinction ratio (ER). However, this is not ideal when 'v' states with an attenuation of around 6 dB are desired, because the voltage fluctuations will cause large deviations in the power that are dependent on the previous level. To get around this patterning effect, it would be better to operate the intensity modulator at two levels, with the device designed such that

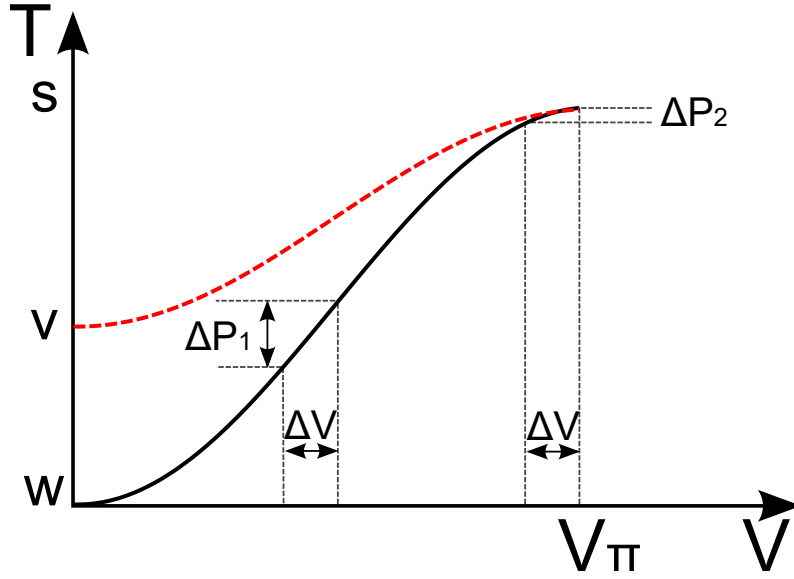


Fig. 5.10 **IM Response.** Transmission ( $T$ ) with voltage ( $V$ ) for an interferometer-based intensity modulator. Power deviations for identical voltage shifts ( $\Delta V$ ) at the peak ( $\Delta P_2$ ) and quadrature point ( $\Delta P_1$ ) are given. The red dotted line shows the output of a low extinction ratio interferometer.

the ER can be chosen arbitrarily, as shown by the red dotted line in Fig. 1b. This means that regardless of the intensity required, it would be possible to operate the device at its half-wave voltage and faithfully produce the desired intensity levels. This technique works because the intensity of the light output from one arm of interferometer-based intensity modulators is

$$I \propto R^2 + T^2 + 2RT \cos(\Delta\phi) \quad (5.25)$$

where  $R : T$  is the coupling ratio of the interfering beam splitter(s),  $R + T = 1$  and  $\Delta\phi$  is the difference in phase between the two pulses when they recombine. This allows the ER, expressed in dB, to be calculated using  $-10\log_{10}(I_{min}/I_{max})$ , where  $I_{min}$  and  $I_{max}$  are obtained from Eq. 5.25 by setting  $\Delta\phi$  to 0 or  $\pi$ , respectively. The result as a function of  $R$  is

$$ER_{max} = -20\log_{10}(|2R - 1|). \quad (5.26)$$

The ER can be chosen to suit the desired application by using a fixed beamsplitter, or it can be tuned with a variable beamsplitter. The aforementioned commercial intensity modulators are designed to target an infinite extinction ratio, which is obtained for  $R = 0.5$ . In reality, however, the splitting ratio is never exactly 0.5 and realistic values are between 20 and 30 dB.

Intensity modulators based on Sagnac interferometers work on a similar principle to MZMs, as shown in Fig. 5.11 [179]. The light is again split into two separate paths, denoted as ‘parallel’ and ‘anti-parallel’, in relation to the propagation direction of the modulating electrical travelling wave. A travelling-wave phase modulator applies a phase shift to the ‘parallel’ wave, meaning the intensity of output light can be controlled. The major difference from an MZM is that the two light pulses travel through the same length of fibre in a short period of time. This means that any perturbations to the fiber, or changes to the DC of the phase modulator, affect both pulses equally. This inherent feature of the modulator means that the device can be very stable and does not require feedback routines [180].

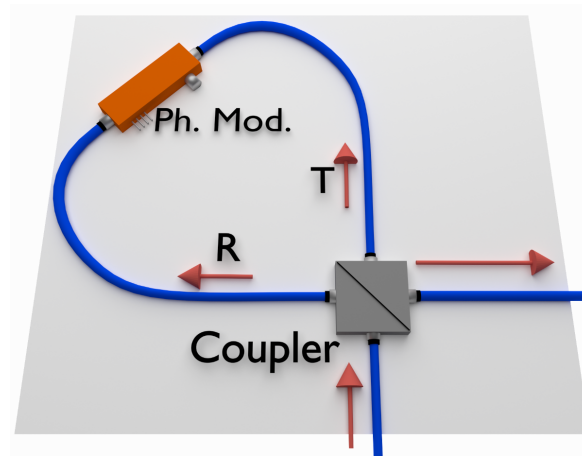


Fig. 5.11 **Sagnac IM.** Schematic of the Sagnac-based intensity modulator with a coupling ratio  $R:T$ .

To demonstrate their operation, 61.5 ps light pulses from the optically injection locked 2 GHz gain switched laser diode described in previous chapters are input to the Sagnac intensity modulator shown in Fig. 5.11. The modulator attenuates or blocks light with no electrical input, so 125 ps electrical pulses are input to the phase modulator when a signal pulse is desired. The electrical pulse delay is tuned so the electrical and light pulses align. A  $2^{10}$ -bit pseudorandom pattern is generated and the corresponding electrical pattern is applied to the phase modulator. Short subsets of the resulting outputs are shown in Fig. 5.12 for beamsplitters with different coupling ratios. Three beamsplitters are tested, with nominal splitting ratios of 50:50, 75:25 and 80:20, but realistically providing ERs of 30.48 dB, 5.83 dB and 3.94 dB respectively at their half-wave voltage.

An analysis of the patterning effects for the Sagnac interferometers with a  $2^{10}$ -bit pseudo-random pattern is shown in Table 5.1. Whilst the modulator can be used to produce vacuum states, the lower optical power pulses are referred to as decoy pulses for all coupling ratios.

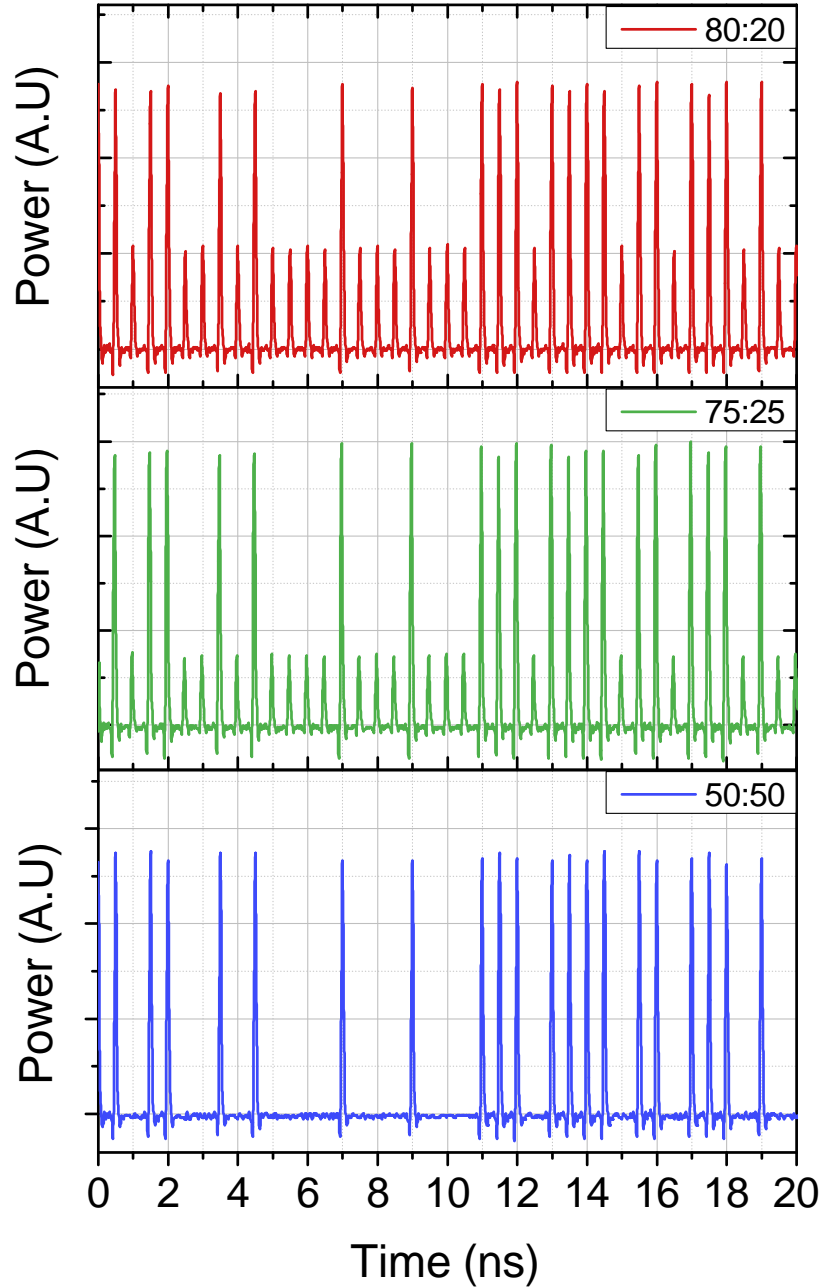


Fig. 5.12 **Oscilloscope traces.** The traces at the maximum ERs are shown for a random input pattern for three different beamsplitters.

The transitions to ‘v’ states are not shown for the 50:50 beamsplitter because the photodiode cannot accurately measure such a high ER. The patterning effects are negligible for all pulse combinations in all three intensity modulators. This is especially obvious when compared to the best case scenario of -18.2% deviation observed by Yoshino *et al.* [178] when producing decoy states using a commercial MZM at the quadrature point. The improvement with



the Sagnac comes from working only at two levels, as shown in Fig. 5.10, but also on the independence of the modulator on electrical DC drifts.

**Table 5.1 External patterning effects.** *The pulse intensities extracted from a  $2^{10}$ -bit pseudorandom pattern input to Sagnac intensity modulators with three different beamsplitting ratios when preceded by a decoy pulse ('v') or another signal pulse ('s'). The average 's' pulse intensity is normalised to unity for each beamsplitter.*

Coupling ratio	Pattern	Average intensity of second pulse	Deviation from average (%)
80:20	s→s	$0.999 \pm 0.021$	0.08
	v→s	$1.001 \pm 0.021$	-0.08
	s→v	$0.403 \pm 0.009$	0.03
	v→v	$0.404 \pm 0.009$	-0.03
75:25	s→s	$0.998 \pm 0.017$	0.20
	v→s	$1.002 \pm 0.017$	-0.19
	s→v	$0.261 \pm 0.006$	0.02
	v→v	$0.262 \pm 0.006$	-0.03
50:50	s→s	$0.999 \pm 0.013$	0.06
	v→s	$1.001 \pm 0.013$	-0.06

The difference in stability between a Sagnac intensity modulator with an 80:20 beamsplitter and a commercial MZM is shown in Fig. 5.13. A power meter with a 1 s averaging time is used to measure the output power for modulators with no applied AC. The Sagnac output shows a Gaussian variation about the mean, with a 1.4 % standard deviation. The DC of the MZM is tuned to provide a similar ER to the Sagnac intensity modulator, left for a day to thermally stabilize, and then is left with no feedback. The output power of the MZM varies unpredictably over a large range of values due to drift, giving a 61.2 % standard deviation. The finite variation of the Sagnac modulator is explained by a misalignment of the phase modulator crystal axis causing mixing between orthogonal polarizations. This is confirmed experimentally by a small observed dependence of the Sagnac output power on the applied DC. The variation could be reduced further by manufacturing a phase modulator with no misalignment.

With regard to modulator design, the ideal case is where the phase modulator is placed asymmetrically in the Sagnac loop. When placed in the center, the 'parallel' light pulse has an interaction length of the whole phase modulator because of the co-propagating electrical pulse, whereas the 'anti-parallel' light is also modulated by the counter-propagating electrical pulse, albeit with a much smaller interaction length. A carefully designed offset from the centre ensures the 'anti-parallel' light does not interact with the electrical pulse. At

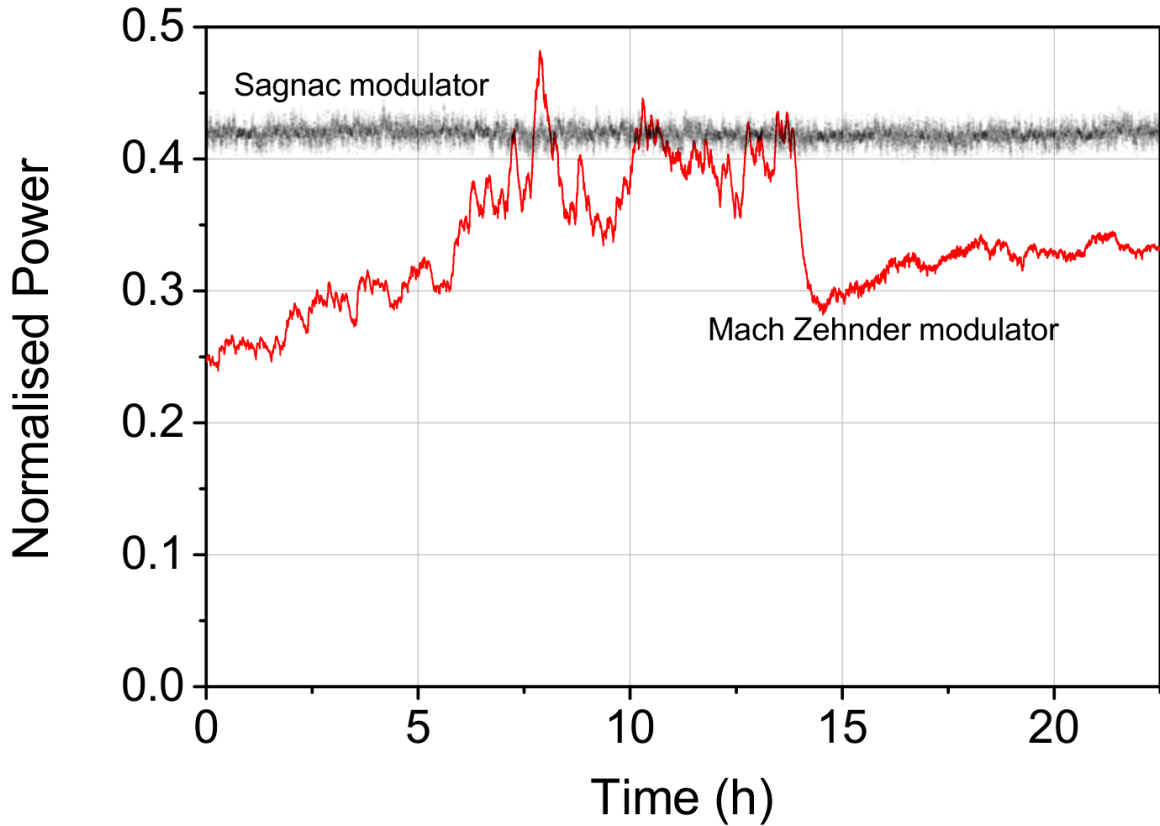


Fig. 5.13 **Temporal stability.** *The output power from an unmodulated Mach Zehnder intensity modulator and the 80:20 Sagnac intensity modulator with no feedback. The power is normalised so the maximum power output is unity.*

higher clock rates this interaction is unavoidable, regardless of the system design, leading to a slightly higher half-wave voltage for the Sagnac intensity modulator than that of the phase modulator. If the input clock rate is too high, however, patterning effects will start to emerge because multiple ‘anti-parallel’ light pulses will be modulated by a single counter-propagating electrical pulse. This limits the maximum clock rate to 3 GHz for ordinary bulk phase modulators with a crystal length of 5 cm, however can be much higher if smaller phase modulators are used [181].

With regard to how this device could be implemented in a QKD system, two decoy-state QKD would require two Sagnac intensity modulators to remove the patterning effects. Fortunately, the modulator stability would mean that this does not add too much complexity to the system. Even still, using as few components as possible would be ideal. One way this could be done is with a single decoy-state QKD protocol, which would require just a single intensity modulator [80, 182]. In fact, the Sagnac intensity modulator is ideal to produce the

decoy states with the directly-modulated quantum transmitter. This transmitter could produce the signal and vacuum states, requiring just a single intensity modulator for the decoy states.

### 5.4.3 Concurrent phase and intensity modulation

Bringing the previously demonstrated direct phase and intensity modulation together to provide concurrent modulation is simple. The phase preparation laser is modulated in the same way as for the phase-encoded BB84 implementation. The laser is driven above threshold to encode a phase shift between two slave laser pulses, before being driven below threshold for a short period of time to randomise the next pulse pair. The pulse preparation laser is patterned in the same way as the COW implementation. The electrical signal into both lasers must then be carefully aligned so the different encoding methods overlap at the correct time.

The transmission probabilities for each basis are set to  $P_Z = 0.8$  and  $P_X = P_Y = 0.1$  and the pulse intensities probabilities are set to  $P_s = 0.8$  and  $P_v = P_w = 0.1$ . All three bases are measured separately, allowing the results to be separated and normalised in post-processing for a comparison between phase-encoded and polar BB84. The actual pulse intensities are  $s = 0.5$  photons per pulse,  $v = 0.038$  photons per pulse and  $w = 0.001$  photons per pulse. Data is measured for 20 minutes in each basis, giving 40 minutes of acquisition for each two-basis protocol. These quantities allow a large number of single photons to be used for the key, whilst obtaining a large sample size for the minority bases and intensities to keep statistical fluctuations low. A  $2^{10}$ -bit pseudorandom pattern is generated to act as the key and the corresponding electrical signal is input to the laser diodes.

In this implementation, the intensity modulator is used solely to produce the decoy states. This minimises the patterning effects because just two levels are modulated. This means that an additional intensity modulator would be required to equalise the mean photon number in the Z basis and X and Y bases. The demonstration is proof of principle, however, meaning this attenuation can simply be moved to the receiver, where a fixed 3 dB attenuation should be added to the X and Y basis receiver. In fact, due to the requirement of basis-independent detection probabilities, 4.7 dB of attenuation is required in the Z-basis, so 1.7 dB of attenuation is experimentally added to the Z basis.

## 5.5 Results and discussion

After tuning the system parameters to minimise the error rate, the optical pulses are sent through a variable optical attenuator to attenuate the pulses to the desired mean photon

number. The pulses are then sent through another variable optical attenuator acting as the quantum channel, or through real optical fibre. A  $2^{11}$ -bin histogram is collected for each distance, allowing the gains and error rate for each basis and intensity to be extracted.

Figure 5.14 shows a 10 ns example from all three measurement bases without any external intensity modulation. Measurement in the Z basis shows the high ER intensity modulation and also shows that there is no difference in intensity between a full pulse followed by a vacuum pulse compared to a full pulse followed by another full pulse. The X and Y basis show a number of different pulse intensities. The maximum and minimum intensity pulses arise when a bit is encoded in that basis. The half-intensity pulses arise either when a bit is encoded in the other phase basis, or due to the random interference between pulses in different blocks. The quarter-intensity pulses are when there is an empty-full pulse sequence in the Z basis.

The worst-case fluctuations of gain and QBER are then calculated using Eq. 5.12. The counts are shown in Fig. 5.15 (top). As expected, they decrease exponentially with channel loss because the photon number and acquisition time is kept constant. The error rates are shown in Fig. 5.15 (bottom). The 2.6 percentage point reduction in error rate of the Z basis compared to the X and Y will allow fewer bits to be used in the error correction process, increasing the secure key rate.

The security parameters  $\epsilon_{sec}$  and  $\epsilon_{cor}$  are set to  $2 \times 10^{-11}$  and  $1 \times 10^{-15}$  respectively. The lower bound on secure key rate can be found using Eq. 5.13. The key rates for polar BB84 are shown in Fig. 5.16. Here, a 1.26 Mbit/s secure key rate can be distilled at 40 km using an attenuator, and 246 kbit/s in real fibre of length 75 km. A positive secure key rate could be achieved up to 250 km in the asymptotic limit. The finite-key-size analysis reduces the secure key rate to zero at around 35 dB with 40 minutes of key time. At 38 dB channel attenuation, just over 1000 counts are observed for the decoy states in the minority basis, which gives too much statistical variation in the counts and error rate. This could be extended simply by obtaining a larger block size.

To compare between polar and phase-encoded BB84, the secure key rate is calculated in the asymptotic limit using the experimental parameters obtained in the ZX and YX bases respectively. The counts are renormalised according to the transmission basis probabilities to allow for a fair comparison. The key rate is improved by 1.60 times when using the ZX basis compared to the YX basis. Also, phase-encoded BB84 is able to reach an attenuation of 48.5 dB with a positive secure key rate, whereas polar BB84 can reach slightly further, at 50.1 dB.

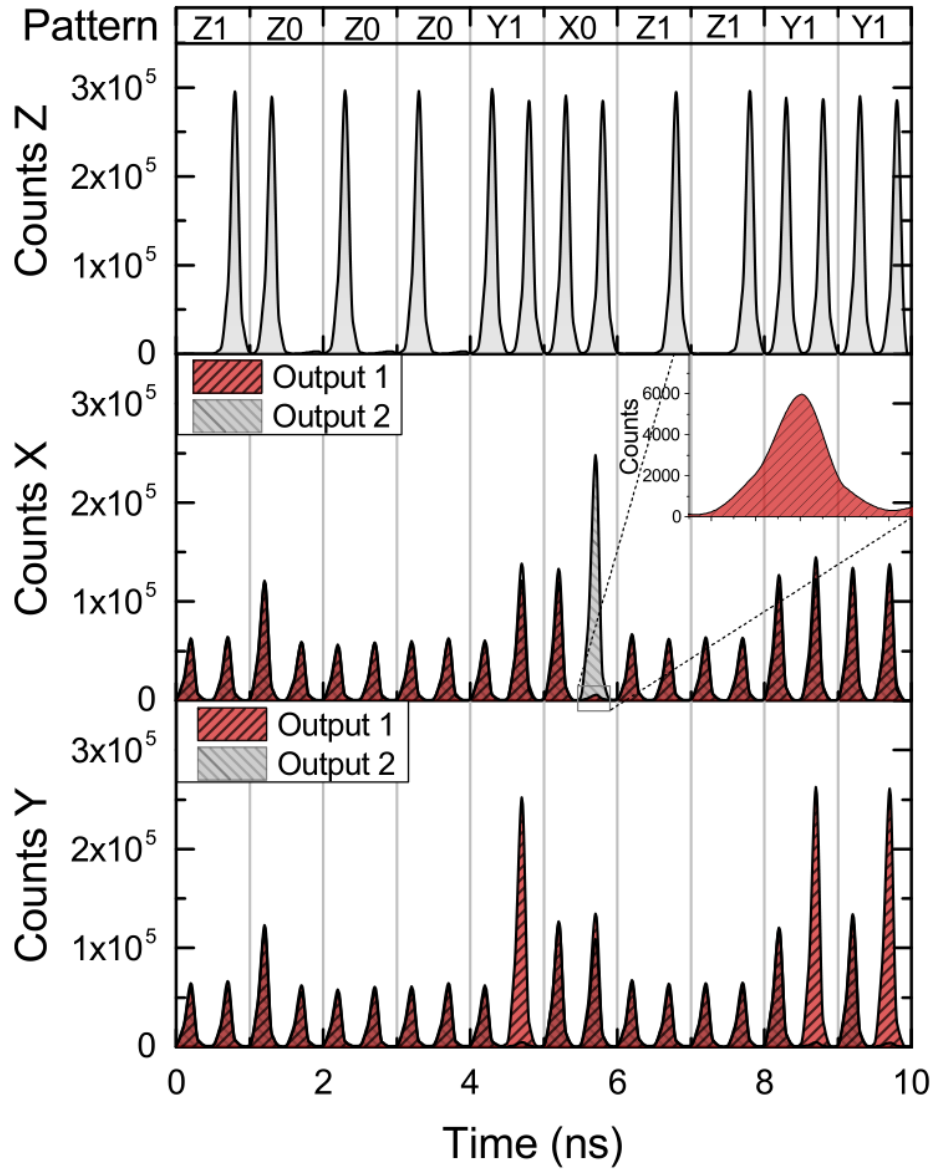


Fig. 5.14 **Six directly-modulated states traces.** *Measurement traces without decoy state preparation and basis intensity equalisation. The Z basis (top) has only a single trace, whereas the X and Y bases (middle and bottom) each have two AMZI outputs. The corresponding input pattern values are displayed at the top, labelled as  $Bb$ , where  $B$  is the basis and  $b$  is the logical bit value inside that basis. A red (grey) peak in the X and Y bases correspond to a '0' ('1') logical bit, where the photon exits through the upper (lower) AMZI port. Peaks in output 1 (2) of the AMZI are complemented by small counts in output 2 (1) (middle inset), showing the high distinguishability between bits.*

Although these results show polar BB84 outperforming phase-encoded BB84, it is not necessarily better to implement polar BB84. There is indeed the benefit of being able to use

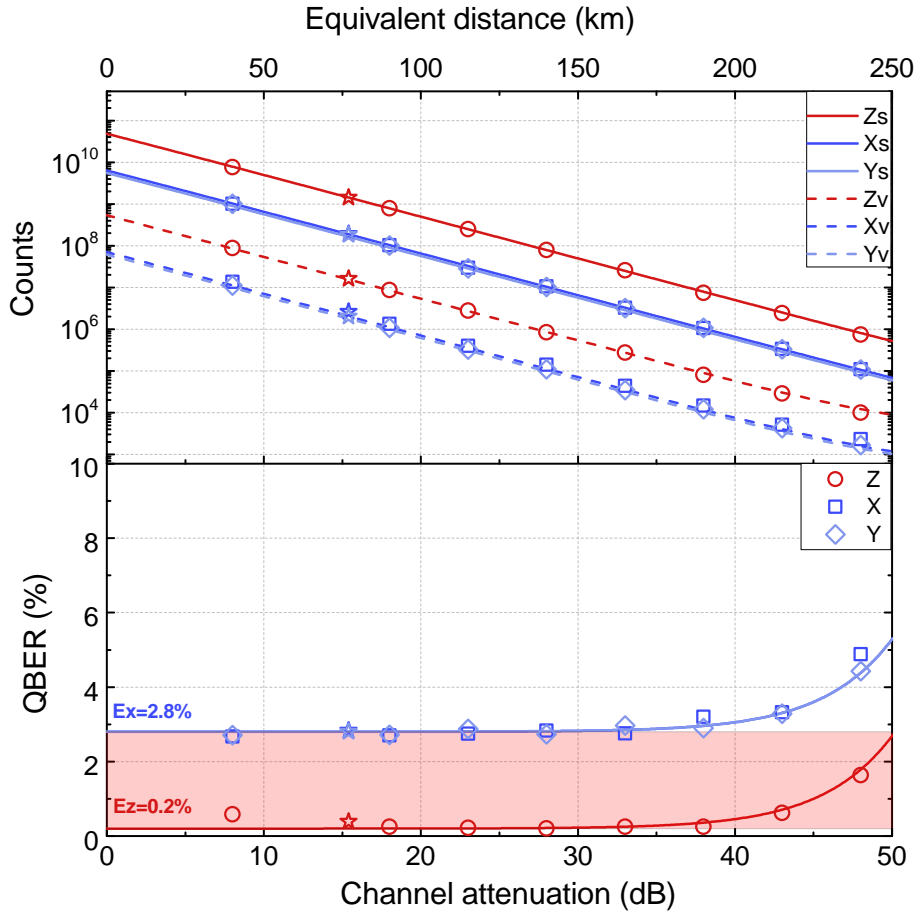


Fig. 5.15 **Experimental counts and error rates.** *The raw counts for each matched basis and intensity for the 20 minutes acquisition time (top) and the corresponding measured QBER (bottom). Lines give the simulation results, stars give the experimental results in real fibre and all other symbols give the experimental results with an attenuator as the optical channel.*

just three SPDs in a passive receiver for polar BB84, compared to four in phase-encoded BB84. In an active implementation, however, phase-encoded BB84 could be carried out using just two SPDs, with a phase modulator in Bob's interferometer. The improvement the directly-modulated transmitter has over a standard transmitter for polar BB84 is marginal. If a different intensity modulator is required for each intensity level, the directly-modulated transmitter would require two intensity modulators, whereas the standard transmitter would require three. This is because the vacuum level can be modulated directly in the former transmitter. Although the intensity encoding used in polar BB84 provides a higher secure key rate, the phase-encoded BB84 protocol could be implemented with a single intensity modulator for the directly-modulated transmitter.

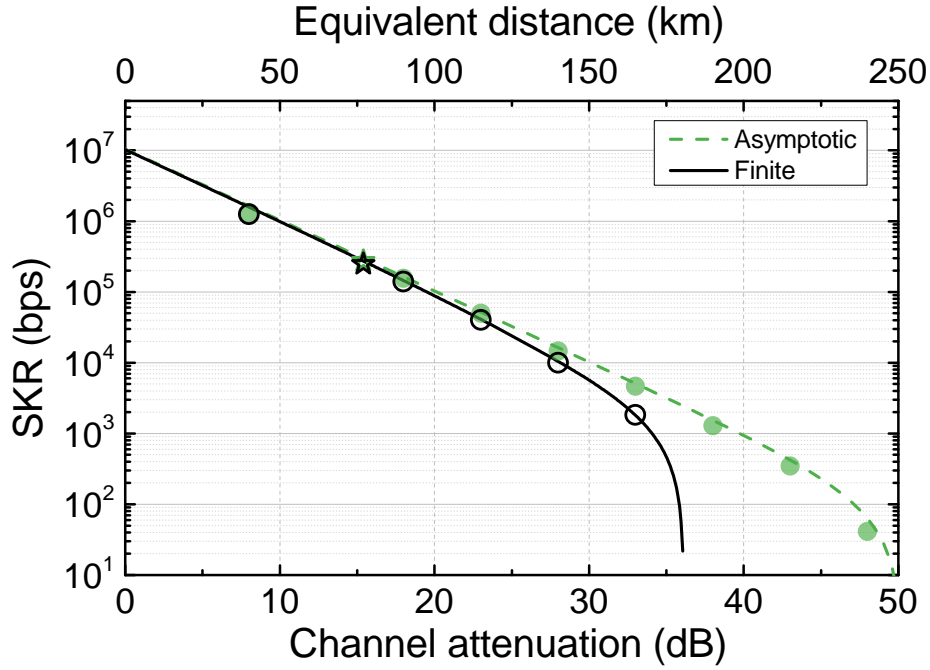


Fig. 5.16 **Polar BB84 Results.** Secure key rate (SKR) in the asymptotic (filled symbols, dotted line) and finite-key-size regimes (empty symbols, solid line). The star corresponds to data collected with real fibre as the quantum channel.

One potential improvement would be the theoretical development of a protocol based on polar BB84. This protocol would have signal states transmitted solely in the X or Y bases, with decoy states transmitted solely in the Z basis. The transmitter inherently emits the Z basis with one half the intensity of the X and Y bases, thus this protocol could retain the benefits of decoy-state QKD, whilst requiring no external modulators.

As mentioned in Section 5.3.2, six-state QKD is also a potential protocol that could be implemented. Unfortunately, however, the increase in secure key rate is very small, especially considering the extra complexity of the receiver. Also, the impact of finite-key-size fluctuations was shown to be the limiting factor in polar BB84, which will only be worse if more time is used to transmit and receive two extra states.

The transmitter also shows promise to be useful in classical communications. The patterning effects that proved prohibitive for QKD when directly producing multiple intensity states are not a major concern here, it will just add a slight degradation to the distinguishability between states. Different intensities can be produced directly, and also a vacuum state can be produced, increasing the amount of information encoded per symbol. The direct modulation means that the system is not reliant on multiple external modulators, making it cheaper, less complex and also easier to integrate with other components. The optical injection locking

also ensures that all pulses have the same wavelength. This removes a side channel for QKD, but also means the system has low chirp, reducing the intersymbol interference caused by dispersion effects. This thesis has shown the accurate production of four phase states because that is all that is required for QKD protocols, however more phase states can be encoded by using more phase-preparation levels.

## 5.6 Summary

This chapter has explored the potential of concurrent phase and intensity modulation with the directly-modulated quantum transmitter. Firstly, decoy states were discussed. Here, three different intensity states are transmitted by Alice, allowing QKD secure key rates to overcome the poor scaling with distance. These would ordinarily be produced using an intensity modulator, so direct modulation of these states would simplify the QKD transmitter. Whilst it was possible to create states with similar spectra, unfortunately the decoy states had intensity fluctuations over 10 %, and also the decoy states are offset from the signal states by 30 ps. This enables Eve to perform a sophisticated attack that removes the benefit of using the decoy states.

Next, decoy state preparation using an external IM was described. Whilst QKD applications usually use MZM-based IMs, they have the drawback of being unstable and can have large patterning effects. For this reason, a two-level Sagnac interferometer is built and tested. This interferometer shows no patterning effects when operated at the maximum and minimum transmission and the ER can be varied by choosing the correct coupler for the interferometer. This modulator also has the advantage of being inherently stable because it utilises a common-path interferometer.

Finally, polar-BB84 was introduced. This is identical to phase-encoded BB84, except it uses the Z-basis with either the X or Y basis. Implementation of this requires concurrent intensity and phase modulation, alongside phase randomisation. The techniques used in the previous chapters are combined to enable this with the directly-modulated quantum transmitter, then data is obtained for 20 minutes in each measurement basis. The Z basis error rate of 0.2 %, compared to the X and Y bases error rates of 2.8 %, means that fewer bits are lost to error correction in polar BB84 than phase-encoded BB84. An asymptotic analysis shows that the secure key rate of polar BB84 is 1.60 times higher than in phase-encoded BB84. A finite-key-size analysis is also carried out for the polar BB84 protocol. This shows secure key rates up to 35 dB channel attenuation, with megabit per second rates below 8 dB channel attenuation. It was also shown that the directly modulated transmitter shows no



---

patterning effects, meaning that the same intensity pulse can be produced regardless of the intensity of the previous pulse.



# Chapter 6

## Future work

The ability of the directly-modulated transmitter to adapt to a number of different QKD protocols has been demonstrated in this thesis. Further experiments and research should help to demonstrate its real world practicality.

Side channel attacks have been described throughout this thesis. It would be valuable to perform a full analysis of the system and identify any weaknesses. One example of an attack on the BB84 protocol implementation would be to inject a large amount of light from the quantum channel into the system. This could have the effect of raising the master laser above threshold during the phase randomisation modulation, essentially ensuring that there is no phase randomisation between different blocks. As described in the thesis, this has the potential to dramatically reduce the secure key rate. A simple countermeasure to this attack is to cascade optical isolators, however an analysis of how the attack affects the system would show whether this countermeasure is necessary.

It is time-consuming to perform different experimental analyses on the system. It would therefore be very useful if an accurate simulation could be built, making searches over large parameter spaces feasible. As an example, it would be interesting to identify the maximum clock rate that the system can work at. In practice this would require a new interferometer, which could be expensive and take a long time to deliver or build. The simulation would allow this to be determined rapidly, accounting for the finite modulation bandwidth of system components.

There is also the potential for a new decoy-state protocol that is particularly adapted to this transmitter. The work in Chapter 5 showed that polar BB84 would require two external intensity modulators in order to stop patterning effects. This is because the X or Y-basis states have to be attenuated by 3 dB so they contain the same number of photons as the Z-basis states. One way to get around this would be to develop a QKD protocol that uses the

X or Y-basis as signal states and the Z-basis as the decoy states. If this protocol were to be developed, it would be trivial to demonstrate experimental modulator-free decoy-state QKD.

New protocols based on weak coherent pulses are still being proposed. One example, the differential phase-time QKD protocol [183] has the potential to offer higher secure key rates compared to other distributed phase reference protocols, because two bits of information are encoded per detection event. The transmitter is able to fulfil all the requirements of this protocol, so it would be interesting to compare how it performs experimentally against the other established QKD protocols. The same could be done for other QKD protocols based on weak coherent pulses as they are published.

Receivers can often be expensive and complex, so it is likely that a user will have a system that can only work with certain QKD protocols. It is also likely, depending on the detectors used, that the receiver clock rate will vary between users. There is nothing stopping the directly-modulated transmitter working at different clock rates because the electrical signal into the lasers can be changed arbitrarily. The effect of a different clock rate on the QBER would be interesting to explore.

Further to this, it would also be desirable for the transmitter to rapidly switch between different QKD protocols. This would allow for a quantum network where keys could be distributed to different users as they are required with little downtime. This experiment would require field-programmable gate arrays to provide the modulations to the lasers and also feedback to the lasers to ensure the setup is optimal. This is necessary because the voltage applied to the lasers can change depending on the protocol, for example the DC voltage is lower for the BB84 protocol to enable phase randomisation, which changes the temperature of the laser, meaning the locking needs to be re-calibrated.

These two developments would pave the way for implementation of the transmitter in a real quantum network. This could be implemented using the ‘metro’ network link in Cambridge between the Electrical Engineering Division in West Cambridge, the Department of Engineering in the city centre and Toshiba Research Europe Limited in the Cambridge Science Park. This work would validate the claim that the transmitter could become the future transmitter in quantum networks.

# Chapter 7

## Conclusions

QKD is a practical technology that allows two users to securely exchange a key using weak laser pulses. According to quantum mechanics, a measurement on the single photon component of these pulses will disturb the photon. This means that if Alice is sending weak laser pulses to Bob, they can determine if an eavesdropper is present because she will introduce errors when she performs a measurement.

The field is currently at the stage where many laboratory and real-world implementations have been demonstrated. QKD has been shown over real optical fibre networks with a high rate, and over a distance of 1200 km using satellites. The technology is reaching the point where researchers and companies have to think about how the technology could be implemented in practical real-world quantum networks.

Differential phase encoding is a popular technique for QKD because it is tolerant to dephasing and polarisation drift in optical fibres. This can be implemented using an external phase modulator to control the phase of light pulses. Instead of this, phase modulation is performed directly in this thesis. One laser is directly modulated to change its phase evolution (the phase preparation laser), before being injected into a pulsed laser (the pulse preparation laser). These pulses then adopt the phase of the first laser. A half-wave voltage of 0.35 V has been demonstrated, the first demonstration of a sub-volt phase modulator, and an order of magnitude lower than commercial phase modulators, which have half-wave voltages around 4-6 V. Whilst the direct method is more power efficient, one benefit of using a commercial phase modulator is that higher clock rates can be reached. The directly-modulated transmitter is limited by the optical bandwidth of the master laser, which is around 10 GHz, whereas commercial phase modulators can reach clock rates of 40 GHz. The complexity of the systems is comparable: direct modulation requires two lasers connected by a circulator, whereas external modulation requires a laser and a phase modulator.

Phase randomisation is also required in some QKD protocols, for example BB84 and DQPS. There are currently two ways of realising this in QKD systems. The first can be used in BB84, and splits phase randomised pulses into an early and late time bin, encoding a differential phase between the two. The difficulty with this solution is maintaining the delay length of the interferometer used to split the pulses, a problem that requires complex feedback mechanisms. The second method is to use a phase modulator and a random number generator. This is more complicated than the first solution, however, requiring infinitely precise electrical modulation signals and a high-speed random number generator. In this thesis, global phase randomisation is made possible at 2 GHz by driving the phase preparation laser below threshold for 125 ps.

The decoy-state technique is a method that has allowed QKD with weak coherent pulses to have the same scaling with channel loss as QKD with single photon sources. This is because an accurate bound can be placed on the number of single photons measured by Bob. Without the decoy-state technique, Alice and Bob would have to assume that all of Bob's clicks could have originated from a multi-photon preparation in Alice. In ordinary QKD systems, the decoy-state technique requires an external intensity modulator to selectively attenuate pulses to different mean photon numbers. Recent work has shown that the most common intensity modulator used, a Mach-Zehnder modulator, can introduce 'patterning effects'. This is where the pulse intensities are correlated, revealing extra information to an eavesdropper. Also, these modulators are temporally unstable and prone to DC drift. In order to remove this side channel and instability, a two-level intensity modulator based on a Sagnac interferometer is proposed. Working at the half-wave voltage of the modulator and changing the beamsplitting ratio ensures that the patterning effects are minimal. Also, the common path interferometer guarantees stability and independence to DC drift. Unfortunately, because only two levels are modulated, two intensity modulators would ordinarily be required for decoy-state QKD with a traditional transmitter. This disadvantage is not true for phase-encoded BB84 with the directly-modulated transmitter, because the vacuum states can be directly modulated. This would then require just a single intensity modulator to provide the decoy states.

The ability to perform phase and intensity modulation allows a fair comparison of multiple QKD protocols from a single transmitter. This is shown in Fig. 7.1. The DPS protocol has the best performance, with almost a 3 dB improvement over the COW and polar decoy-state BB84 protocols. This is mainly due to the DPS protocol having double the effective clock rate because every time bin is useful. Also, there is only a single measurement basis so there is no sifting loss because Alice and Bob never have mismatched bases. Finally, the DPS protocol does not require decoy states like the other two, meaning the single photon yield

for the key is higher. The COW protocol is unable to reach the same distances as the DPS and polar decoy-state BB84 protocols. This is because only 10 % of the pulses received by Bob are used to measure the visibility, meaning dark counts are much more of an issue. This could be improved by changing the beamsplitting ratio, however it would decrease the secure key rate at short distances. It is also important to note that the polar decoy-state BB84 protocol is the only one of the three with security against coherent attacks. The DQPS and phase-encoded BB84 protocols have a worse scaling with channel transmittance because the mean photon number must be decreased as the channel length increases. This leads to their secure key rates being worse at all distances, and also they can only reach half the distance of the DPS and polar decoy-state protocols.

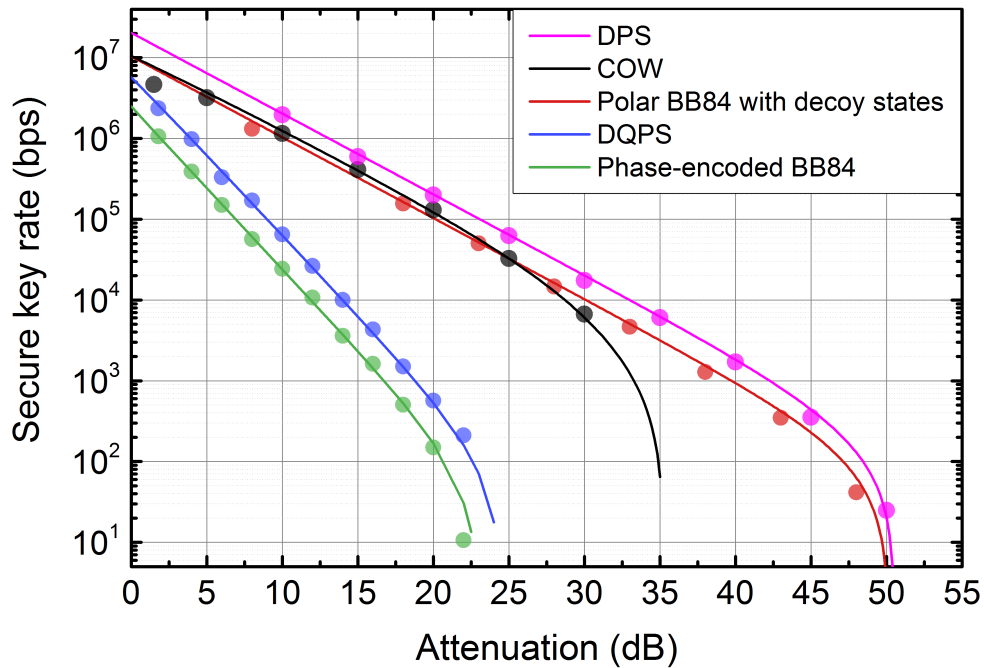


Fig. 7.1 **All protocols key rates.** Asymptotic secure key rates for all QKD protocols implemented in this thesis.

This transmitter has great potential to be used in a quantum communication network. Although the comparison figure shows some protocols outperforming others, this does not account for differences in the receiver complexity, or the security level of the protocols. These factors will cause users to implement different protocols depending on their requirements. Having a simple transmitter that can adapt to the receiver is therefore a highly desirable property, allowing users to communicate indiscriminately with all receivers.





# References

- [1] W. B. Jones, *Introduction to optical fiber communication systems*. Holt, Rinehart & Winston, 1988.
- [2] K. Shaneman and S. Gray, “Optical network security: technical analysis of fiber tapping mechanisms and methods for detection & prevention,” in *Military Communications Conference, 2004. MILCOM 2004. 2004 IEEE*, vol. 2, pp. 711–716, IEEE, 2004.
- [3] A. J. Menezes, J. Katz, P. C. v. Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, Oct. 1996.
- [4] M. Willett, “Cryptography old and new,” *Computers & Security*, vol. 1, no. 2, pp. 177–186, 1982.
- [5] D. Kahn, *The codebreakers*. Weidenfeld and Nicolson, 1974.
- [6] D. Dolev and A. C. Yao, “On the security of public key protocols,” *Information Theory, IEEE Transactions on*, vol. 29, no. 2, pp. 198–208, 1983.
- [7] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.
- [8] M. Bellare and P. Rogaway, “The exact security of digital signatures-How to sign with RSA and Rabin,” in *Advances in Cryptology Eurocrypt 96*, pp. 399–416, Springer, 1996.
- [9] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.
- [10] J. C. A. v. d. Lubbe, *Basic Methods of Cryptography*. Cambridge University Press, Mar. 1998.
- [11] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, “Towards practical and fast quantum cryptography,” *arXiv preprint quant-ph/0411022*, 2004.
- [12] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” *Rev. Mod. Phys.*, vol. 81, no. 3, p. 1301, 2009.

- [13] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *International Conference on Computer System and Signal Processing, IEEE, 1984*, pp. 175–179, 1984.
- [14] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, Oct. 1982.
- [15] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters*, vol. 68, no. 21, p. 3121, 1992.
- [16] R. Etengu, F. M. Abbou, H. Y. Wong, A. Abid, N. Nortiza, and A. Setharaman, "Performance Comparison of BB84 and B92 Satellite-Based Free Space Quantum Optical Communication Systems in the Presence of Channel Effects," *Journal of Optical Communications*, vol. 32, Jan. 2011.
- [17] A. Poppe, A. Fedrizzi, R. Ursin, H. R. Boehm, T. Lorunser, O. Maurhardt, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, and A. Zeilinger, "Practical quantum key distribution with polarization entangled photons," *Optics Express*, vol. 12, pp. 3865–3871, 2004.
- [18] X. Ma, C.-H. F. Fung, and H.-K. Lo, "Quantum key distribution with entangled photon sources," *Physical Review A*, vol. 76, July 2007.
- [19] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Physical review letters*, vol. 70, no. 13, p. 1895, 1993.
- [20] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical review letters*, vol. 67, no. 6, p. 661, 1991.
- [21] A. Ling, M. Peloso, I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer, "Experimental E91 quantum key distribution," in *Advanced Optical Concepts in Quantum Computing, Memory, and Communication* (Z. U. Hasan, A. E. Craig, and P. R. Hemmer, eds.), vol. 69030, SPIE, Feb. 2008.
- [22] Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Avoiding the blinding attack in QKD," *Nature Photonics*, vol. 4, p. 800, Dec. 2010.
- [23] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs, "Attacks on practical quantum key distribution systems (and how to prevent them)," *Contemporary Physics*, vol. 57, pp. 366–387, July 2016.
- [24] A. Koehler-Sidki, J. F. Dynes, M. Lucamarini, G. L. Roberts, A. W. Sharpe, Z. L. Yuan, and A. J. Shields, "Best-Practice Criteria for Practical Security of Self-Differencing Avalanche Photodiode Detectors in Quantum Key Distribution," *Physical Review Applied*, vol. 9, Apr. 2018.
- [25] H.-K. Lo, M. Curty, and B. Qi, "Measurement-Device-Independent Quantum Key Distribution," *Physical Review Letters*, vol. 108, Mar. 2012.

- [26] R. Valivarthi, I. Lucio-Martinez, P. Chan, A. Rubenok, C. John, D. Korchinski, C. Duffin, F. Marsili, V. Verma, M. D. Shaw, and others, “Measurement device independent quantum key distribution: from idea towards application,” *Journal of Modern Optics*, vol. 62, no. 14, pp. 1141–1150, 2015.
- [27] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, “Making the decoy-state measurement-device-independent quantum key distribution practically useful,” *Physical Review A*, vol. 93, Apr. 2016.
- [28] C. K. Hong, Z. Y. Ou, and L. Mandel, “Measurement of subpicosecond time intervals between two photons by interference,” *Physical Review Letters*, vol. 59, no. 18, p. 2044, 1987.
- [29] G. Weihs and others, “Photonic entanglement for fundamental tests and quantum communication,” *arXiv preprint quant-ph/0107156*, 2001.
- [30] G. L. Roberts, M. Lucamarini, Z. L. Yuan, J. F. Dynes, L. C. Comandar, A. W. Sharpe, A. J. Shields, M. Curty, I. V. Puthoor, and E. Andersson, “Experimental measurement-device-independent quantum digital signatures,” *Nature Communications*, vol. 8, no. 1, 2017.
- [31] K. Inoue, E. Waks, and Y. Yamamoto, “Differential Phase Shift Quantum Key Distribution,” *Physical Review Letters*, vol. 89, p. 037902, June 2002.
- [32] K. Inoue and T. Honjo, “Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack,” *Physical Review A*, vol. 71, p. 042305, Apr. 2005.
- [33] C. Branciard, N. Gisin, and V. Scarani, “Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography,” *New Journal of Physics*, vol. 10, no. 1, p. 013031, 2008.
- [34] H.-W. Li, Z.-Q. Yin, S. Wang, W. Chen, Z.-F. Han, W.-S. Bao, and G.-C. Guo, “Lower bounds for the security of modified coherent-one-way quantum key distribution against one-pulse-attack,” *Optics Communications*, vol. 284, no. 3, pp. 889–892, 2011.
- [35] T. Moroder, M. Curty, C. C. W. Lim, L. P. Thinh, H. Zbinden, and N. Gisin, “Security of Distributed-Phase-Reference Quantum Key Distribution,” *Physical Review Letters*, vol. 109, Dec. 2012.
- [36] M. Mafu, A. Marais, and F. Petruccione, “A Necessary Condition for the Security of Coherent-One-Way Quantum Key Distribution Protocol,” *Appl. Math*, vol. 8, no. 6, pp. 2769–2773, 2014.
- [37] T. C. Ralph, “Continuous variable quantum cryptography,” *Physical Review A*, vol. 61, no. 1, p. 010303, 1999.
- [38] W. Hu, D. Shu, D. Wang, and Y. Liu, “Principles and improvements of quadrature-based QKD,” in *Quantum and Nonlinear Optics* (Q. Gong, G.-C. Guo, and Y.-R. Shen, eds.), (Beijing, China), p. 78460, SPIE, Nov. 2010.

- [39] X. Zhang, Y. Zhang, Z. Li, S. Yu, and H. Guo, “1.2 GHz Balanced Homodyne Detector for Continuous-Variable Quantum Information Technology,” *arXiv:1806.09393 [physics, physics:quant-ph]*, June 2018.
- [40] N. Gisin and R. T. Thew, “Quantum communication technology,” *Electronics letters*, vol. 46, no. 14, pp. 965–967, 2010.
- [41] N. Cerf and P. Grangier, “Quantum cloning and key distribution with continuous variables,” in *Quantum Information Processing and Communications (QPIC) in Europe*, European Commission, 2005.
- [42] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, “Quantum key distribution using gaussian-modulated coherent states,” *Nature*, vol. 421, no. 6920, pp. 238–241, 2003.
- [43] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, “Continuous-Variable Quantum Key Distribution with Gaussian Modulation—The Theory of Practical Implementations,” *Advanced Quantum Technologies*, p. 1800011, 2018.
- [44] A. Leverrier, “Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States,” *Physical Review Letters*, vol. 114, Feb. 2015.
- [45] D. Huang, D. Lin, C. Wang, W. Liu, S. Fang, J. Peng, P. Huang, and G. Zeng, “Continuous-variable quantum key distribution with 1 Mbps secure key rate,” *Optics Express*, vol. 23, p. 17511, June 2015.
- [46] D. Huang, P. Huang, D. Lin, and G. Zeng, “Long-distance continuous-variable quantum key distribution by controlling excess noise,” *Scientific Reports*, vol. 6, p. 19201, Jan. 2016.
- [47] H. Zbinden, N. Gisin, B. Huttner, A. Muller, and W. Tittel, “Practical Aspects of Quantum Cryptographic Key Distribution,” *Journal of Cryptology*, vol. 13, pp. 207–220, Mar. 2000.
- [48] E. Waks, H. Takesue, and Y. Yamamoto, “Security of differential-phase-shift quantum key distribution against individual attacks,” *Physical Review A*, vol. 73, p. 012344, Jan. 2006.
- [49] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, “Practical free-space quantum key distribution over 10 km in daylight and at night,” *New journal of physics*, vol. 4, no. 1, p. 43, 2002.
- [50] J. Wabnig, D. Bitauld, H. W. Li, A. Laing, J. L. O’Brien, and A. O. Niskanen, “Demonstration of free-space reference frame independent quantum key distribution,” *New Journal of Physics*, vol. 15, p. 073001, July 2013.
- [51] S.-K. Liao, H.-L. Yong, C. Liu, G.-L. Shentu, D.-D. Li, J. Lin, H. Dai, S.-Q. Zhao, B. Li, J.-Y. Guan, W. Chen, Y.-H. Gong, Y. Li, Z.-H. Lin, G.-S. Pan, J. S. Pelc, M. M. Fejer, W.-Z. Zhang, W.-Y. Liu, J. Yin, J.-G. Ren, X.-B. Wang, Q. Zhang, C.-Z. Peng, and J.-W. Pan, “Long-distance free-space quantum key distribution in daylight towards inter-satellite communication,” *Nature Photonics*, vol. 11, pp. 509–513, July 2017.

- [52] R. Bedington, J. M. Arrazola, and A. Ling, “Progress in satellite quantum key distribution,” *npj Quantum Information*, vol. 3, no. 1, 2017.
- [53] “1 Mbps coherent one-way QKD with dense wavelength division multiplexing and hardware key distillation,” Lecture notes in computer science, (Berlin), Springer, 2012.
- [54] K. Patel, J. Dynes, M. Lucamarini, I. Choi, A. Sharpe, Z. Yuan, R. Penty, and A. Shields, “Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks,” *Applied Physics Letters*, vol. 104, no. 5, p. 051123, 2014.
- [55] K. Takemoto, Y. Nambu, T. Miyazawa, Y. Sakuma, T. Yamamoto, S. Yorozu, and Y. Arakawa, “Quantum key distribution over 120 km using ultrahigh purity single-photon source and superconducting single-photon detectors,” *Scientific Reports*, vol. 5, p. 14383, Sept. 2015.
- [56] N. Lütkenhaus, “Security against individual attacks for realistic quantum key distribution,” *Physical Review A*, vol. 61, p. 052304, Apr. 2000.
- [57] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, “Limitations on Practical Quantum Cryptography,” *Physical Review Letters*, vol. 85, pp. 1330–1333, Aug. 2000.
- [58] N. Lütkenhaus and M. Jahma, “Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack,” *New Journal of Physics*, vol. 4, pp. 44–44, July 2002.
- [59] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, “Security of Quantum Key Distribution with Imperfect Devices,” *Quantum Info. Comput.*, vol. 4, pp. 325–360, Sept. 2004.
- [60] Z.-F. Han, X.-F. Mo, Y.-Z. Gui, and G.-C. Guo, “Stability of phase-modulated quantum key distribution systems,” *Applied Physics Letters*, vol. 86, no. 22, p. 221103, 2005.
- [61] R. Goldstein, “Electro-optic devices in review,” *Lasers & Applications*, Apr. 1986.
- [62] E. L. Wooten, K. M. Kissa, A. Yi-Yan, E. J. Murphy, D. A. Lafaw, P. F. Hallemeier, D. Maack, D. V. Attanasio, D. J. Fritz, G. J. McBrien, and others, “A review of lithium niobate modulators for fiber-optic communications systems,” *IEEE Journal of selected topics in Quantum Electronics*, vol. 6, no. 1, pp. 69–82, 2000.
- [63] R. S. Weis and T. K. Gaylord, “Lithium niobate: summary of physical properties and crystal structure,” *Applied Physics A*, vol. 37, no. 4, pp. 191–203, 1985.
- [64] K. Hinton, G. Raskutti, P. M. Farrell, and R. S. Tucker, “Switching energy and device size limits on digital photonic signal processing technologies,” *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 14, no. 3, pp. 938–945, 2008.
- [65] J. E. Toney, *Lithium Niobate Photonics*. Artech House, July 2015.
- [66] Y. Enami, C. T. Deroose, D. Mathine, C. Loychik, C. Greenlee, R. A. Norwood, T. D. Kim, J. Luo, Y. Tian, A. K.-Y. Jen, and N. Peyghambarian, “Hybrid polymer/sol–gel waveguide modulators with exceptionally large electro–optic coefficients,” *Nature Photonics*, vol. 1, pp. 180–185, Mar. 2007.

- [67] C. Hunziker, S.-J. Kwon, H. Figi, M. Jazbinsek, and P. Gunter, “Fabrication and phase modulation in organic single-crystalline configurationally locked, phenolic polyene OH1 waveguides,” *Optics express*, vol. 16, no. 20, pp. 15903–15914, 2008.
- [68] Z. Yang, L. Mutter, M. Stillhart, B. Ruiz, S. Aravazhi, M. Jazbinsek, A. Schneider, V. Gramlich, and P. Günter, “Large-Size Bulk and Thin-Film Stilbazolium-Salt Single Crystals for Nonlinear Optics and THz Generation,” *Advanced Functional Materials*, vol. 17, pp. 2018–2023, Sept. 2007.
- [69] H. Inamori, N. Lütkenhaus, and D. Mayers, “Unconditional security of practical quantum key distribution,” *The European Physical Journal D*, vol. 41, p. 599, Mar. 2007.
- [70] Y. Zhao, B. Qi, and H.-K. Lo, “Experimental quantum key distribution with active phase randomization,” *Applied physics letters*, vol. 90, no. 4, pp. 656–661, 2007.
- [71] H.-K. Lo and J. Preskill, “Security of quantum key distribution using weak coherent states with nonrandom phases,” *Quantum Information & Computation*, vol. 8, pp. 431–458, 2007.
- [72] H.-K. Lo and J. Preskill, “Phase randomization improves the security of quantum key distribution,” *arXiv preprint quant-ph/0504209*, 2005.
- [73] F. James, “A review of pseudorandom number generators,” *Computer Physics Communications*, vol. 60, no. 3, pp. 329–344, 1990.
- [74] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, “A statistical test suite for random and pseudorandom number generators for cryptographic applications,” tech. rep., Booz-Allen and Hamilton Inc Mclean Va, 2001.
- [75] J. Kelsey, B. Schneier, D. Wagner, and C. Hall, “Cryptanalytic attacks on pseudorandom number generators,” in *Fast Software Encryption*, pp. 168–188, Springer, 1998.
- [76] M. Matsumoto, M. Saito, H. Haramoto, and T. Nishimura, “Pseudorandom Number Generation: Impossibility and Compromise,” *J. UCS*, vol. 12, no. 6, pp. 672–690, 2006.
- [77] M. Herrero-Collantes and J. C. Garcia-Escartin, “Quantum random number generators,” *Reviews of Modern Physics*, vol. 89, no. 1, p. 015004, 2017.
- [78] Z. Yuan, M. Lucamarini, J. Dynes, B. Fröhlich, A. Plews, and A. Shields, “Robust random number generation using steady-state emission of gain-switched laser diodes,” *Applied Physics Letters*, vol. 104, no. 26, p. 261112, 2014.
- [79] D. G. Marangon, A. Plews, M. Lucamarini, J. F. Dynes, A. W. Sharpe, Z. Yuan, and A. J. Shields, “Long-Term Test of a Fast and Compact Quantum Random Number Generator,” *Journal of Lightwave Technology*, vol. 36, pp. 3778–3784, Sept. 2018.
- [80] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, “Practical decoy state for quantum key distribution,” *Physical Review A*, vol. 72, p. 012326, July 2005.

- [81] V. Scarani and R. Renner, “Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Postprocessing,” *Physical Review Letters*, vol. 100, May 2008.
- [82] R. Y. Cai and V. Scarani, “Finite-key analysis for practical implementations of quantum key distribution,” *New Journal of Physics*, vol. 11, no. 4, p. 045024, 2009.
- [83] L. Sheridan, T. P. Le, and V. Scarani, “Finite-key security against coherent attacks in quantum key distribution,” *New Journal of Physics*, vol. 12, p. 123019, Dec. 2010.
- [84] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, “Tight finite-key analysis for quantum cryptography,” *Nature Communications*, vol. 3, p. 634, Jan. 2012.
- [85] S. Kawakami, T. Sasaki, and M. Koashi, “Finite-key analysis for quantum key distribution with weak coherent pulses based on Bernoulli sampling,” *Physical Review A*, vol. 96, July 2017.
- [86] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, “Provably secure and practical quantum key distribution over 307 km of optical fibre,” *Nature Photonics*, vol. 9, no. 3, pp. 163–168, 2015.
- [87] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, “Concise security bounds for practical decoy-state quantum key distribution,” *Physical Review A*, vol. 89, p. 022307, Feb. 2014.
- [88] R. H. Hadfield, “Single-photon detectors for optical quantum information applications,” *Nature Photonics*, vol. 3, pp. 696–705, Dec. 2009.
- [89] Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields, “High speed single photon detection in the near-infrared,” *arXiv preprint arXiv:0707.4307*, 2007.
- [90] A. W. Ziarkash, S. K. Joshi, M. Stipčević, and R. Ursin, “Comparative study of afterpulsing behavior and models in single photon counting avalanche photo diode detectors,” *Scientific Reports*, vol. 8, p. 5076, Mar. 2018.
- [91] C. M. Natarajan, M. G. Tanner, and R. H. Hadfield, “Superconducting nanowire single-photon detectors: physics and applications,” *Superconductor Science and Technology*, vol. 25, p. 063001, June 2012.
- [92] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, “Detecting single infrared photons with 93% system efficiency,” *Nature Photonics*, vol. 7, pp. 210–214, Feb. 2013.
- [93] H. Shibata, K. Fukao, N. Kirigane, S. Karimoto, and H. Yamamoto, “SNSPD With Ultimate Low System Dark Count Rate Using Various Cold Filters,” *IEEE Transactions on Applied Superconductivity*, vol. 27, pp. 1–4, June 2017.
- [94] D. Rosenberg, A. E. Lita, A. J. Miller, and S. W. Nam, “Noise-free high-efficiency photon-number-resolving detectors,” *Physical Review A*, vol. 71, no. 6, p. 061803, 2005.

- [95] A. E. Lita, A. J. Miller, and S. W. Nam, "Counting near-infrared single-photons with 95% efficiency," *Optics Express*, vol. 16, pp. 3032–3040, Mar. 2008.
- [96] L. Comandar, B. Fröhlich, M. Lucamarini, K. Patel, A. Sharpe, J. Dynes, Z. Yuan, R. Penty, and A. Shields, "Room temperature single-photon detectors for high bit rate quantum key distribution," *Applied Physics Letters*, vol. 104, no. 2, p. 021101, 2014.
- [97] N. Namekata and S. Inoue, "Ultra-low-noise high-speed single-photon detection using a sinusoidally gated InGaAs/InP avalanche photodiode," vol. 7945, International Society for Optics and Photonics, Jan. 2011.
- [98] N. Walenta, T. Lunghi, O. Guinnard, R. Houlmann, H. Zbinden, and N. Gisin, "Sine gating detector with simple filtering for low-noise infra-red single photon detection at room temperature," *Journal of Applied Physics*, vol. 112, no. 6, p. 063106, 2012.
- [99] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. Sharpe, A. Dixon, E. Lavelle, J. Dynes, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato, and A. J. Shields, "10-Mb/s Quantum Key Distribution," *Journal of Lightwave Technology*, vol. 36, pp. 3427–3433, Aug. 2018.
- [100] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussi eres, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Secure quantum key distribution over 421 km of optical fiber," *arXiv:1807.03222 [quant-ph]*, July 2018.
- [101] B. Fr hlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, and A. J. Shields, "Long-distance quantum key distribution secure against coherent attacks," *Optica*, vol. 4, p. 163, Jan. 2017.
- [102] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, "Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber," *Physical Review Letters*, vol. 117, p. 190501, Nov. 2016.
- [103] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA Quantum Network," *arXiv:quant-ph/0503058*, Mar. 2005.
- [104] M. Peev, C. Pacher, R. All aume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. F rst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. H bel, G. Humer, T. L nger, M. Legr , R. Lieger, J. Lodewyck, T. Lor nser, N. L tkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouiri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The SECOQC quantum key distribution network in Vienna," *New Journal of Physics*, vol. 11, p. 075001, July 2009.
- [105] A. Mirza and F. Petruccione, "Realizing long-term quantum cryptography," *JOSA B*, vol. 27, pp. A185–A188, June 2010.



- [106] D. Stucki, M. Legré, L. Monat, S. Robyr, P. Trinkler, G. Ribordy, R. Thew, N. Walenta, N. Gisin, F. Buntschu, D. Perroud, G. Litzistorf, J. Tavares, S. Ventura, P. Junod, R. Vioir, and P. Monbaron, “Performance of the SwissQuantum network over 21 months,” p. 81891D, Oct. 2011.
- [107] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, “Field test of quantum key distribution in the Tokyo QKD Network,” *Optics Express*, vol. 19, p. 10387, May 2011.
- [108] S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, H. Chen, Y.-G. Han, J.-Z. Huang, J.-F. Guo, P.-L. Hao, M. Li, C.-M. Zhang, D. Liu, W.-Y. Liang, C.-H. Miao, P. Wu, G.-C. Guo, and Z.-F. Han, “Field and long-term demonstration of a wide area quantum key distribution network,” *Optics Express*, vol. 22, pp. 21739–21756, Sept. 2014.
- [109] A. Wonfor, H. Qin, R. Kumar, X. Tang, J. F. Dynes, A. J. Shields, R. V. Penty, and I. H. White, “Field trial of a QKD and high-speed classical data hybrid metropolitan network (Conference Presentation),” in *SPIE, Broadband Access Communication Technologies XII* (B. B. Dingel, K. Tsukamoto, and S. Mikroulis, eds.), (San Francisco), p. 1055907, SPIE, Mar. 2018.
- [110] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, “Satellite-to-ground quantum key distribution,” *Nature*, vol. 549, pp. 43–47, Aug. 2017.
- [111] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O’Brien, and M. G. Thompson, “Chip-based quantum key distribution,” *Nature Communications*, vol. 8, p. 13984, Feb. 2017.
- [112] J. L. Duligall, M. S. Godfrey, K. A. Harrison, W. J. Munro, and J. G. Rarity, “Low cost and compact quantum key distribution,” *New Journal of Physics*, vol. 8, pp. 249–249, Oct. 2006.
- [113] H. Chun, I. Choi, G. Faulkner, L. Clarke, B. Barber, G. George, C. Capon, A. Niskanen, J. Wabnig, D. O’Brien, and D. Bitauld, “Handheld free space quantum key distribution with dynamic motion compensation,” *Optics Express*, vol. 25, pp. 6784–6795, Mar. 2017.
- [114] G. Mélen, P. Freiwang, J. Luhn, T. Vogl, M. Rau, C. Sonnleitner, W. Rosenfeld, H. Weinfurter, and H. Weinfurter, “Handheld Quantum Key Distribution,” in *Quantum*

- Information and Measurement (QIM) 2017, QT6A.57*, Optical Society of America, Apr. 2017.
- [115] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, “Overcoming the rate–distance limit of quantum key distribution without quantum repeaters,” *Nature*, vol. 557, p. 400, May 2018.
  - [116] X. Ma, P. Zeng, and H. Zhou, “Phase-matching quantum key distribution,” *arXiv:1805.05538 [quant-ph]*, May 2018.
  - [117] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, “Sending or not sending: twin-field quantum key distribution with large misalignment error,” *arXiv:1805.09222 [quant-ph]*, May 2018.
  - [118] X.-B. Wang, X.-L. Hu, and Z.-W. Yu, “Effective Eavesdropping to Twin Field Quantum Key Distribution,” *arXiv:1805.02272 [quant-ph]*, May 2018.
  - [119] K. Tamaki, H.-K. Lo, W. Wang, and M. Lucamarini, “Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound,” *arXiv:1805.05511 [quant-ph]*, May 2018.
  - [120] R. Kingston, H., *Optical sources, detectors, and systems: Fundamentals and applications*. Optics and Photonics, Academic press, 1995.
  - [121] D. M. Pataca, P. Gunning, M. L. Rocha, J. K. Lucek, R. Kashyap, K. Smith, D. G. Moodie, R. P. Davey, R. F. Souza, and A. S. Siddiqui, “Gain-switched DFB lasers,” *Journal of Microwaves, Optoelectronics and Electromagnetic Applications (JMoe)*, vol. 1, no. 1, pp. 46–63, 1997.
  - [122] A. E. Siegman, *Lasers*. University Science Books, 1986.
  - [123] M. Bennett, M. F. Schatz, H. Rockwood, and K. Wiesenfeld, “Huygens’s clocks,” *Proceedings: Mathematics, Physical and Engineering Sciences*, pp. 563–579, 2002.
  - [124] R. Adler, “A Study of Locking Phenomena in Oscillators,” *Proceedings of the IRE*, vol. 34, pp. 351–357, June 1946.
  - [125] R. Lang, “Injection locking properties of a semiconductor laser,” *IEEE Journal of Quantum Electronics*, vol. 18, pp. 976–983, June 1982.
  - [126] E. K. Lau, L. J. Wong, and M. C. Wu, “Enhanced modulation characteristics of optical injection-locked lasers: A tutorial,” *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 15, no. 3, p. 618, 2009.
  - [127] C. Lin and F. Mengel, “Reduction of frequency chirping and dynamic linewidth in high-speed directly modulated semiconductor lasers by injection locking,” *Electronics Letters*, vol. 20, pp. 1073–1075, Dec. 1984.
  - [128] X. J. Meng, T. Chau, and M. C. Wu, “Improved intrinsic dynamic distortions in directly modulated semiconductor lasers by optical injection locking,” *IEEE Transactions on Microwave Theory and Techniques*, vol. 47, pp. 1172–1176, July 1999.

- [129] N. Olsson and J. V. D. Ziel, "Performance characteristics of 1.5- $\mu\text{m}$  external cavity semiconductor lasers for coherent optical communication," *Journal of Lightwave Technology*, vol. 5, pp. 510–515, Apr. 1987.
- [130] E. K. Lau, X. Zhao, H.-K. Sung, D. Parekh, C. Chang-Hasnain, and M. C. Wu, "Strong optical injection-locked semiconductor lasers demonstrating greater 100-GHz resonance frequencies and 80-GHz intrinsic bandwidths," *Optics Express*, vol. 16, no. 9, pp. 6609–6618, 2008.
- [131] J. M. Sarraute, K. Schires, S. LaRochelle, and F. Grillot, "Enhancement of the Modulation Dynamics of an Optically Injection-Locked Semiconductor Laser Using Gain Lever," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, pp. 575–582, Nov. 2015.
- [132] X. Jin and S. L. Chuang, "Relative intensity noise characteristics of injection-locked semiconductor lasers," *Applied Physics Letters*, vol. 77, pp. 1250–1252, Aug. 2000.
- [133] J. Poette, O. Vaudel, and P. Besnard, "Relative intensity noise of an injected semiconductor laser," pp. 605407–605407–10, Dec. 2005.
- [134] C. E. Webb and J. D. C. Jones, *Handbook of Laser Technology and Applications: Laser design and laser systems*. CRC Press, 2004.
- [135] D.-S. Seo, D. Y. Kim, and H.-F. Liu, "Timing jitter reduction of gain-switched DFB laser by external injection-seeding," *Electronics Letters*, vol. 32, pp. 44–45, Jan. 1996.
- [136] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W.-B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Quantum key distribution without detector vulnerabilities using optically seeded lasers," *Nature Photonics*, vol. 10, pp. 312–315, Apr. 2016.
- [137] J.-D. Deschênes, L. C. Sinclair, F. R. Giorgetta, W. C. Swann, E. Baumann, H. Bergeron, M. Cermak, I. Coddington, and N. R. Newbury, "Synchronization of Distant Optical Clocks at the Femtosecond Level," *Physical Review X*, vol. 6, May 2016.
- [138] A. H. Zewail, "Femtochemistry: Atomic-Scale Dynamics of the Chemical Bond," *The Journal of Physical Chemistry A*, vol. 104, pp. 5660–5694, June 2000.
- [139] M. Hentschel, B. Schrenk, R. Lieger, E. Querasser, and H. Hübel, "Low-Cost Single-Laser Differential Phase Shift Transmitter Towards SFP-based QKD Tail-End Optics," in *QCrypt 2017*, (Cambridge), 2017.
- [140] Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, M. B. Ward, and A. J. Shields, "Interference of short optical pulses from independent gain-switched laser diodes for quantum secure communications," *Physical Review Applied*, vol. 2, no. 6, p. 064006, 2014.
- [141] A. Strecok, "On the calculation of the inverse of the error function," *Mathematics of Computation*, vol. 22, pp. 144–144, Jan. 1968.
- [142] E. Ip, A. P. T. Lau, D. J. F. Barros, and J. M. Kahn, "Coherent detection in optical fiber systems," *Optics Express*, vol. 16, no. 2, p. 753, 2008.

- [143] K. Inoue, E. Waks, and Y. Yamamoto, "Differential-phase-shift quantum key distribution using coherent light," *Physical Review A*, vol. 68, p. 022317, Aug. 2003.
- [144] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors," *Nature Photonics*, vol. 1, pp. 343–348, June 2007.
- [145] N. Namekata, H. Takesue, T. Honjo, Y. Yokura, and Inoue, "High-rate quantum key distribution over 100 km using ultra-low-noise, 2-GHz sinusoidally gated InGaAs/InP avalanche photodiodes," *Optics Express*, vol. 19, no. 11, p. 10632, 2011.
- [146] S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han, "2 GHz clock quantum key distribution over 260 km of standard telecom fiber," *Optics Letters*, vol. 37, pp. 1008–1010, Mar. 2012.
- [147] K. Inoue, "Differential Phase-Shift Quantum Key Distribution Systems," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, pp. 109–115, May 2015.
- [148] H. Shibata, T. Honjo, and K. Shimizu, "Quantum key distribution over a 72 dB channel loss using ultralow dark count superconducting single-photon detectors," *Optics Letters*, vol. 39, p. 5078, Sept. 2014.
- [149] H. Takesue, E. Diamanti, C. Langrock, M. M. Fejer, and Y. Yamamoto, "10-GHz clock differential phase shift quantum key distribution experiment," *Optics Express*, vol. 14, pp. 9522–9530, Oct. 2006.
- [150] T. Sasaki, Y. Yamamoto, and M. Koashi, "Practical quantum key distribution protocol without monitoring signal disturbance," *Nature*, vol. 509, pp. 475–478, May 2014.
- [151] B. Fröhlich and Z. Yuan, "Quantum cryptography: Round-robin with photons," *Nature Photonics*, vol. 9, no. 12, pp. 781–782, 2015.
- [152] Y.-H. Li, Y. Cao, H. Dai, J. Lin, Z. Zhang, W. Chen, Y. Xu, J.-Y. Guan, S.-K. Liao, J. Yin, Q. Zhang, X. Ma, C.-Z. Peng, and J.-W. Pan, "Experimental round-robin differential phase-shift quantum key distribution," *Physical Review A*, vol. 93, Mar. 2016.
- [153] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, "Experimental quantum key distribution without monitoring signal disturbance," *Nat Photon*, vol. 9, pp. 827–831, Dec. 2015.
- [154] S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, X.-T. Song, H.-W. Li, L.-J. Zhang, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Experimental demonstration of a quantum key distribution without signal disturbance monitoring," *Nature Photonics*, vol. 9, pp. 832–836, Nov. 2015.
- [155] J.-Y. Guan, Z. Cao, Y. Liu, G.-L. Shen-Tu, J. S. Pelc, M. M. Fejer, C.-Z. Peng, X. Ma, Q. Zhang, and J.-W. Pan, "Experimental passive round-robin differential phase-shift quantum key distribution," *Physical review letters*, vol. 114, no. 18, p. 180502, 2015.
- [156] S. Kawakami, T. Sasaki, and M. Koashi, "Security of the differential-quadrature-phase-shift quantum key distribution," *Physical Review A*, vol. 94, Aug. 2016.

- [157] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, “Continuous operation of high bit rate quantum key distribution,” *Applied Physics Letters*, vol. 96, p. 161102, Apr. 2010.
- [158] A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M. J. Li, D. Nolan, A. Martin, and H. Zbinden, “Simple 2.5 GHz time-bin quantum key distribution,” *arXiv preprint arXiv:1804.05426*, 2018.
- [159] N. Calandri, Q.-Y. Zhao, D. Zhu, A. Dane, and K. K. Berggren, “Superconducting nanowire detector jitter limited by detector geometry,” *Applied Physics Letters*, vol. 109, p. 152601, Oct. 2016.
- [160] L. Goleniewski, *Telecommunications essentials: the complete global source for communications fundamentals, data networking and the Internet, and next-generation networks*. Addison-Wesley Professional, 2002.
- [161] M. Nakazawa, S. Okamoto, T. Omiya, K. Kasai, and M. Yoshida, “256-QAM (64 Gb/s) Coherent Optical Transmission Over 160 km With an Optical Bandwidth of 5.4 GHz,” *IEEE Photonics Technology Letters*, vol. 22, pp. 185–187, Feb. 2010.
- [162] G. Ungerboeck, “Channel coding with multilevel/phase signals,” *IEEE Transactions on Information Theory*, vol. 28, pp. 55–67, Jan. 1982.
- [163] Y. Nambu, K. Yoshino, and A. Tomita, “Quantum encoder and decoder for practical quantum key distribution using a planar lightwave circuit,” *Journal of Modern Optics*, vol. 55, pp. 1953–1970, July 2008.
- [164] M. Koashi, “Efficient quantum key distribution with practical sources and detectors,” *arXiv:quant-ph/0609180*, Sept. 2006.
- [165] W.-Y. Hwang, “Quantum Key Distribution with High Loss: Toward Global Secure Communication,” *Physical Review Letters*, vol. 91, p. 057901, Aug. 2003.
- [166] H.-K. Lo, X. Ma, and K. Chen, “Decoy State Quantum Key Distribution,” *Physical Review Letters*, vol. 94, p. 230504, June 2005.
- [167] X.-B. Wang, “Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography,” *Physical Review Letters*, vol. 94, p. 230503, June 2005.
- [168] M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, “Efficient decoy-state quantum key distribution with quantified security,” *Optics Express*, vol. 21, no. 21, p. 24550, 2013.
- [169] M. Lucamarini, J. F. Dynes, B. Frohlich, Zhiliang Yuan, and A. J. Shields, “Security Bounds for Efficient Decoy-State Quantum Key Distribution,” *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, pp. 197–204, May 2015.
- [170] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller, and J. E. Nordholt, “Long-distance quantum key distribution in optical fibre,” *New Journal of Physics*, vol. 8, no. 9, p. 193, 2006.

- [171] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, “Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate,” *Optics Express*, vol. 16, pp. 18790–18797, 2008.
- [172] T.-Y. Chen, H. Liang, Y. Liu, W.-Q. Cai, L. Ju, W.-Y. Liu, J. Wang, H. Yin, K. Chen, Z.-B. Chen, C.-Z. Peng, and J.-W. Pan, “Field test of a practical secure communication network with decoy-state quantum cryptography,” *Optics Express*, vol. 17, p. 6540, Apr. 2009.
- [173] D. Rosenberg, C. G. Peterson, J. W. Harrington, P. R. Rice, N. Dallmann, K. T. Tyagi, K. P. McCabe, S. Nam, B. Baek, R. H. Hadfield, and others, “Practical long-distance quantum key distribution system using decoy levels,” *New Journal of Physics*, vol. 11, no. 4, p. 045009, 2009.
- [174] Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang, and others, “Decoy-state quantum key distribution with polarized photons over 200 km,” *Optics Express*, vol. 18, no. 8, pp. 8587–8594, 2010.
- [175] Y.-y. Fei, X.-d. Meng, M. Gao, Y. Yang, H. Wang, and Z. Ma, “Strong light illumination on gain-switched semiconductor lasers helps the eavesdropper in practical quantum key distribution systems,” *Optics Communications*, vol. 419, pp. 83–89, July 2018.
- [176] A. Huang, S.-H. Sun, Z. Liu, and V. Makarov, “Decoy state quantum key distribution with imperfect source,” *arXiv:1711.00597 [quant-ph]*, Nov. 2017.
- [177] G. Kato and K. Tamaki, “Security of six-state quantum key distribution protocol with threshold detectors,” *Scientific Reports*, vol. 6, p. srep30044, July 2016.
- [178] K.-i. Yoshino, M. Fujiwara, K. Nakata, T. Sumiya, T. Sasaki, M. Takeoka, M. Sasaki, A. Tajima, M. Koashi, and A. Tomita, “Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses,” *npj Quantum Information*, vol. 4, no. 1, 2018.
- [179] X. Fang, H. Ji, L. J. Pelz, K. R. Demarest, and C. Allen, “A DC to multigigabit/s polarization-independent modulator based on a Sagnac interferometer,” *Journal of Lightwave Technology*, vol. 15, pp. 2166–2171, Nov. 1997.
- [180] S. Wang, W. Chen, Z.-Q. Yin, D.-Y. He, C. Hui, P.-L. Hao, G.-J. Fan-Yuan, C. Wang, L.-J. Zhang, J. Kuang, S.-F. Liu, Z. Zhou, Y.-G. Wang, G.-C. Guo, and Z.-F. Han, “Practical gigahertz quantum key distribution robust against channel disturbance,” *Optics Letters*, vol. 43, pp. 2030–2033, May 2018.
- [181] R. Spickermann, S. R. Sakamoto, M. G. Peters, and N. Dagli, “GaAs/AlGaAs traveling wave electro-optic modulator with an electrical bandwidth >40 GHz,” *Electronics Letters*, vol. 32, pp. 1095–1096, June 1996.
- [182] D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, “Finite-key analysis on the 1-decoy state QKD protocol,” *Applied Physics Letters*, vol. 112, p. 171104, Apr. 2018.
- [183] D. Bacco, J. B. Christensen, M. A. U. Castaneda, Y. Ding, S. Forchhammer, K. Rottwitt, and L. K. Oxenløwe, “Two-dimensional distributed-phase-reference protocol for quantum key distribution,” *Scientific Reports*, vol. 6, p. 36756, Dec. 2016.